#2

BUNDESREPUBLIK DEUTSCHLAND

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

EP04/505

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	103 50 647.0
Anmeldetag:	29. Oktober 2003
Anmelder/Inhaber:	Francotyp-Postalia AG & Co KG, 16547 Birkenwerder/DE
Bezeichnung:	Verfahren und Anordnung zur mobilen Datenübertragung
IPC:	H 04 L 9/32

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 12. Februar 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Schäfer

A 9161
06/00
EDV-L

Verfahren und Anordnung zur mobilen Datenübertragung

Die vorliegende Erfindung betrifft ein Verfahren zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung, insbesondere einem Fahrzeug, und einer von der ersten Einrichtung zumindest zeitweise entfernten Datenzentrale, wobei die Übertragung der Daten über wenigstens eine mobile erste Übertragungseinrichtung erfolgt. Sie betrifft weiterhin eine entsprechende Anordnung zum Übertragen von Daten.

Ein solches gattungsgemäßes Verfahren ist beispielsweise aus dem Bereich der Schienenverkehrstechnik bekannt. Dort werden zwischen dem Steuerrechner des Zuges über eine damit verbundene entsprechende Sender/Empfängereinheit des Zuges Daten mit einer externen Zugleitstelle ausgetauscht. Sofern es sich bei den ausgetauschten Daten um sicherheitsrelevante Daten handelt, wird durch entsprechend redundante Übertragungsprotokolle eine fehlerfreie Übertragung der die Daten repräsentierenden Signale sichergestellt bzw. werden nur solche Signale akzeptiert, deren Fehlerwahrscheinlichkeit innerhalb bestimmter Toleranzgrenzen liegt.

Ein Nachteil dieser bekannten Verfahren liegt darin, dass eine Absicherung der durch die Signale repräsentierten Daten gegen Manipulationen in der Regel nicht stattfindet. Bei der Übertragung der Daten zwischen dem Fahrzeug und der Datenzentrale könnte es somit problemlos zu wissentlichen und willentlichen Manipulationen kommen. Dies ist insbesondere dann von Nachteil, wenn diese Daten sicherheitsrelevante erste Daten umfassen. Um hier Manipulationen vorzubeugen, wäre es wünschenswert, eine entsprechende Absicherung solcher sicherheitsrelevanter erster Daten und damit einen Manipulationsschutz zu erzielen.

Weiterhin wäre es wünschenswert, das bekannte Verfahren auch in anderen Bereichen einsetzen zu können. Insbesondere wäre es wünschenswert, ein solches Verfahren bei der Überwachung anderer mobiler Einrichtungen einzusetzen. Hierzu zählt insbesondere die Überwachung von gemieteten oder geleasten Fahrzeugen. Gerade hier stellt sich aber wieder das Problem, dass die übertragenen Daten, gerade wenn sie beispielsweise abrechnungsrelevante und damit sicherheitsrelevante erste Daten umfassen, mit dem bekannten Datenübertragungsverfahren vergleichsweise anfällig für Manipulationen sind.

Der vorliegenden Erfindung liegt daher die Aufgabe zu Grunde, ein Verfahren bzw. eine Anordnung der eingangs genannten Art zur Verfügung zu stellen, welches bzw. welche die oben genannten Nachteile nicht oder zumindest in geringerem Maß aufweist und, insbesondere bei der Übertragung, einen erhöhten Manipulationsschutz sicherheitsrelevanter Daten gewährleistet.

Die vorliegende Erfindung löst diese Aufgabe ausgehend von einem Verfahren gemäß dem Oberbegriff des Anspruchs 1 durch die im kennzeichnenden Teil des Anspruchs 1 angegebenen Merkmale. Sie löst diese Aufgabe weiterhin ausgehend von einer Anordnung gemäß dem Oberbegriff des Anspruchs 17 durch die im kennzeichnenden Teil des Anspruchs 17 angegebenen Merkmale.

Der vorliegenden Erfindung liegt die technische Lehre zu Grunde, dass man einen erhöhten Manipulationsschutz sicherheitsrelevanter erster Daten erzielt, wenn die übertragenen ersten Daten durch kryptographische Mittel authentifiziert werden. Die Authentifizierung bringt den Vorteil mit sich, dass auch zu einem späteren Zeitpunkt durch ein entsprechendes Verifizierungsverfahren zweifelsfrei nachgewiesen werden kann, dass die Daten während der Übertragung oder gegebenenfalls auch später nicht manipuliert wurden.

Die Authentifizierung durch kryptographische Mittel kann in beliebiger bekannter Weise erfolgen. So kann beispielsweise ein so genannter Message Authentification Code (MAC) verwendet werden. Ein solcher MAC wird in der Regel unter Verwendung eines so genannten geteilten Geheimnisses, in der Regel eines geheimen Schlüssels generiert, der sowohl der den MAC erzeugenden Einheit als auch der den MAC verifizierenden Einheit bekannt ist, ansonsten aber geheim gehalten wird. Die zu authentifizierenden Daten werden zusammen mit dem geheimen Schlüssel einem Berechnungsalgorithmus zugeführt, der hieraus den MAC generiert. Der Berechnungsalgorithmus ist so ausgebildet, dass der MAC ohne Kenntnis des geheimen Schlüssels ohne übermäßig hohen Berechnungsaufwand nicht aus den zu authentifizierenden Daten rekonstruiert werden kann. Üblicherweise schließt der Berechnungsalgorithmus einen so genannten Hash-Algorithmus (z. B. SHA-1, SHA-2, MD5 etc.) ein. Zur Verifizierung des MAC wird seitens der verifizierenden Einheit aus den zu authentifizierenden Daten zusammen mit dem geheimen Schlüssel unter Verwendung des selben Berechnungsalgorithmus ein zweiter MAC gebildet, der dann mit dem MAC verglichen wird, der den zu authentifizierenden Daten zugeordnet ist. Stimmen diese überein, sind die Daten authentisch.

Wegen der einfacheren Verwaltung der verwendeten kryptographischen Schlüssel, insbesondere der einfacheren Verteilung der öffentlichen Schlüssel, beispielsweise im Rahmen

einer so genannten Public Key Infrastruktur (PKI), werden zur Authentifizierung der Daten vorzugsweise digitale Signaturen verwendet. Hierbei verschlüsselt die Einheit, welche die digitale Signatur erzeugt, die zu authentifizierenden Daten oder einen daraus generierten Wert mit einem privaten Schlüssel, der in der Regel nur ihr bekannt ist. Um die den zu authentifizierenden Daten zugeordnete Signatur zu verifizieren und damit die Authentizität der Daten zu überprüfen, entschlüsselt die verifizierende Einheit die Signatur mit einem ihr bekannten öffentlichen Schlüssel, der dem privaten Schlüssel zugeordnet ist. Das Ergebnis der Entschlüsselung wird dann mit den zu authentifizierenden Daten oder einem Wert, der daraus nach dem bei der Verschlüsselung verwendeten Algorithmus generiert wurde. Stimmen diese überein, sind die Daten authentisch.

Bei den zu authentifizierenden ersten Daten kann es sich grundsätzlich um beliebige Daten handeln. So kann es sich um beliebige Daten handeln, die von entsprechenden Einrichtungen der ersten Einrichtung bzw. der Datenzentrale erfasst oder generiert wurden. Insbesondere kann es sich um beliebige Daten handeln, die von entsprechenden Erfassungseinrichtungen der mobilen ersten Einrichtung erfasst wurden. Hierzu zählen unter anderem beliebige Messdaten, die über beliebige Messeinrichtungen gemessen wurden.

Vorzugsweise wird zusammen mit diesen Daten auch ihre jeweilige Quelle authentifiziert. Hierzu ist bevorzugt vorgesehen, dass die ersten Daten zur Authentifizierung einer ersten Quelle der ersten Daten wenigstens eine erste Quellenidentifikation umfassen. Diese erste Quellenidentifikation ist der ersten Quelle bevorzugt eindeutig zugeordnet. Es handelt sich vorzugsweise um eine einmalige und eindeutige Identifikation. Bei der ersten Quelle, die über die erste Quellenidentifikation identifiziert wird, kann es sich um die Einrichtung handeln, welche die ersten Daten erfasst bzw. generiert hat. So kann die erste Quelle beispielsweise ein Messaufnehmer oder Sensor sein, der die ersten Daten generiert. Ebenso kann es sich bei der ersten Quelle um eine Einrichtung handeln, über welche die ersten Daten im weiteren Verlauf geleitet werden. Dies ist insbesondere dann sinnvoll, wenn die ersten Daten durch diese Einrichtung eine Bearbeitung, eine Modifikation oder dergleichen erfahren. So kann die erste Quelle beispielsweise die Einrichtung sein, in der die ersten Daten authentifiziert werden. Ebenso kann es sich bei der ersten Quelle um eine Einrichtung handeln, über welche die ersten Daten übertragen werden.

Ein weiterer Vorteil dieser Variante liegt darin, dass durch die eindeutige Zuordnung der Daten zu der jeweiligen ersten Quelle anhand der authentifizierten Daten zu einem späteren Zeitpunkt eine Aussage über die Qualität und die Leistungsfähigkeit der ersten Quelle getroffen werden kann. Dies gilt insbesondere dann, wenn eine längere Reihe von entsprechenden authentifizierten Daten zur Verfügung steht, sodass eine entsprechende Historie über

die Leistung der ersten Quelle erstellt werden kann, aus der entsprechende Rückschlüsse gezogen werden können.

Die erste Quelle kann Bestandteil der ersten Einrichtung, der ersten Übertragungseinrichtung, der Datenzentrale oder jeder weiteren Einrichtung sein, über welche die Datenübertragung erfolgt. Vorzugsweise umfassen die ersten Daten jeweils eine Quellenidentifikation für sämtliche Stationen, welche die ersten Daten bei der Übertragung durchlaufen, um ihren Übertragungsweg zu einem späteren Zeitpunkt lückenlos nachvollziehen zu können.

Bei besonders vorteilhaften Ausgestaltungen des erfindungsgemäßen Verfahrens wird zudem auch der Empfänger der ersten Daten authentifiziert. Hierdurch ist es möglich, zu einem späteren Zeitpunkt den Nachweis zu führen, welche Daten an einen bestimmten Empfänger übergeben wurden. Dies ist insbesondere dann von Bedeutung, wenn der Empfang der ersten Daten die Erfüllung einer bestimmten entgeltpflichtigen Leistung darstellt. Durch die erfindungsgemäße Authentifizierung des Empfängers kann dann in vorteilhafter Weise zu einem späteren Zeitpunkt der Empfänger der ersten Daten und damit der Leistung nachgewiesen werden. Erfindungsgemäß ist hierzu bevorzugt vorgesehen, dass die ersten Daten zur Authentifizierung eines ersten Empfängers der ersten Daten eine erste Empfängeridentifikation umfassen.

Je nach Übertragungsrichtung kann der Empfänger Bestandteil der ersten Einrichtung, der ersten Übertragungseinrichtung, der Datenzentrale oder jeder weiteren Einrichtung sein, über welche die Datenübertragung erfolgt. Analog zu der oben geschilderten Quellenidentifikation ist vorzugsweise vorgesehen, dass die ersten Daten eine Empfängeridentifikation für jeden Empfänger aufweist, über den die Übertragung erfolgt. Bei Zwischenstationen in der Übertragung entspricht die Empfängeridentifikation dann in der Regel der Quellenidentifikation, sodass für solche Zwischenstationen lediglich eine einzige Identifikation in die ersten Daten aufgenommen werden muss.

Bei besonders vorteilhaften Varianten des erfindungsgemäßen Verfahrens wird zusätzlich die Übertragung selbst bzw. ein Merkmal dieser Übertragung authentifiziert. Hierdurch ist es zu einem späteren Zeitpunkt möglich, gegebenenfalls nicht nur die Daten und die beteiligten Kommunikationspartner zweifelsfrei zu identifizieren. Es ist hiermit auch möglich, den Vorgang der Übertragung selbst zu identifizieren und/oder seine Qualität zu bewerten. So kann die Übertragung beispielsweise durch ein entsprechendes zeitliches Merkmal in eine Reihenfolge von Übertragungen eingeordnet werden, um eine Historie der Übertragungen bzw. der übertragenen Daten zu erstellen. Ebenso kann die Übertragung durch ein entsprechendes Qualitätsmerkmal, beispielsweise das Signal-Rausch-Verhältnis, die Anzahl der Verbin-

dungsversuche, Art und/oder Anzahl von aufgetretenen Fehlern etc., später hinsichtlich ihrer Qualität beurteilt werden. Erfindungsgemäß ist hierzu vorgesehen, dass die ersten Daten zur Authentifizierung der Übertragung der ersten Daten eine Übertragungsidentifikation umfassen. Diese Übertragungsidentifikation kann beispielsweise eine fortlaufende Übertragungsnummer umfassen, welche die Übertragung beispielsweise zusammen mit den Identifikationen der Kommunikationspartner eindeutig identifiziert. Eine exakte zeitliche Einordnung der Übertragung ist möglich, wenn die Übertragungsidentifikation eine absolute Zeitinformation hinsichtlich Beginn und/oder Ende der Übertragung umfasst.

Bei weiteren bevorzugten Varianten des erfindungsgemäßen Verfahrens werden zeitliche Ereignisse authentifiziert. Erfindungsgemäß umfassen die ersten Daten hierzu wenigstens eine für ein vorgebbares Ereignis charakteristische Zeitkennung. Bei den vorgebbaren Ereignis kann es sich beispielsweise um die Generierung bzw. Erfassung der zu übertragenen Daten handeln, ebenso kann es sich um das Senden bzw. Empfangen der ersten Daten handeln. Vorzugsweise ist jeweils eine Zeitkennung für einen dieser Vorgänge vorgesehen. Mit anderen Worten umfassen die ersten Daten beispielsweise eine erste Zeitkennung, die für den Zeitpunkt der Generierung bzw. Erfassung der zu übersenden Daten repräsentativ ist, eine zweite Zeitkennung, die für das Senden dieser Daten repräsentativ ist, und eine dritte Zeitkennung, die für das Empfangen dieser Daten repräsentativ ist.

Bei besonders vorteilhaften Varianten des erfindungsgemäßen Verfahrens ist vorgesehen, dass die authentifizierten ersten Daten in einen Protokolldatensatz eingefügt werden, der in der ersten Einrichtung und zusätzlich oder alternativ in der Datenzentrale gespeichert wird. Dieser Protokolldatensatz ermöglicht es gegebenenfalls beiden Kommunikationspartnern ohne weiteres zu einem beliebigen späteren Zeitpunkt die entsprechend authentifizierten Daten zu verifizieren.

Besonders günstige Varianten des erfindungsgemäßen Verfahrens zeichnen sich dadurch aus, dass mit ihnen eine zuverlässige Überwachung bestimmter Zustände, insbesondere bestimmter Zustände der mobilen ersten Einrichtung möglich ist. Erfindungsgemäß ist hierzu vorgesehen, dass die ersten Daten von der ersten Einrichtung zur Datenzentrale übertragene erste Überwachungsdaten umfassen, die wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße umfassen, der von einer ersten Erfassungseinrichtung der ersten Einrichtung erfasst wurde.

Bei der Erfassungsgröße kann es sich grundsätzlich um eine beliebige durch entsprechende Erfassungseinrichtungen erfassende Größe handeln. So kann es sich beispielsweise um eine Zustandgröße der Umgebung der mobilen ersten Einrichtung handeln, welche durch

entsprechende Sensoren oder dergleichen der mobilen ersten Einrichtung erfasst wird. Besonders vorteilhaft lässt sich das erfindungsgemäßen Verfahren jedoch zur Überwachung des Zustands der mobilen Einrichtung selbst einsetzen. Bevorzugt handelt es sich bei der ersten Erfassungsgröße daher um eine Zustandsgröße der ersten Einrichtung. Diese Zustandgröße kann beispielsweise ein Betriebsparameter der ersten Einrichtung sein. Hierzu zählen beispielsweise die Geschwindigkeit und die Beschleunigung der ersten Einrichtung, die nach Betrag und Richtung erfasst werden können. Ebenso kann natürlich auch die Position der ersten Einrichtung die erste Erfassungsgröße bilden. Ebenso kann es sich um eine Temperatur handeln, wie z. B. die Temperatur im Kühlwasser- oder Motorölkreislauf etc. Schließlich kann es sich um einen Ölstand, den Reifendruck oder einen beliebigen anderen Zustandsparameter handeln. Es versteht sich im übrigen, dass beliebige Kombinationen solche Erfassungsgrößen über entsprechende Erfassungseinrichtungen erfasst und übermittelt werden können, um den Zustand der ersten Einrichtung zu charakterisieren.

Weitere vorteilhafte Varianten des erfindungsgemäßen Verfahrens ermöglichen eine Beeinflussung bestimmter Betriebsparameter und damit des Betriebs der mobilen ersten Einrichtung. Erfindungsgemäß ist hierzu vorgesehen, dass die ersten Daten wenigstens Betriebsbeeinflussungsdaten umfassen, die zur Beeinflussung des Betriebs der ersten Einrichtung an die erste Einrichtung übermittelt werden. So ist es beispielsweise möglich, durch die Übertragung der ersten Daten zur ersten Einrichtung aktuelle Betriebsparameter zu verändern. Ebenso kann beispielsweise ein Austausch von Teilen der Betriebssoftware der ersten Einrichtung bis hin zum kompletten Austausch der Betriebssoftware vorgenommen werden. Mit der erfindungsgemäßen Authentifizierung der ersten Daten kann, gegebenenfalls zusammen mit anderen Sicherungsmechanismen, sichergestellt werden, dass nur authentische und autorisierte Daten berücksichtigt werden. Es kann damit also mit anderen Worten nur zu einer autorisierten Beeinflussung des Betriebs der mobilen ersten Einrichtung erfolgen.

Bei weiteren vorteilhaften Varianten des erfindungsgemäßen Verfahrens werden die Daten über wenigstens eine zweite Datenübertragungseinrichtung übertragen. Diese zweite Datenübertragungseinrichtung kann sowohl ebenfalls mobil als auch stationär sein. Hierdurch ist es möglich, ein kostengünstiges Übertragungssystem zu realisieren. So kann die zweite Datenübertragungseinrichtung entsprechend leistungsfähig ausgebildet sein, um die ersten Daten über eine weite Strecke zu und von der Datenzentrale zu übertragen. Die erste Datenübertragungseinrichtung kann dann einfacher und kostengünstiger gestaltet werden. Insbesondere kann sie für eine kürzere Übertragungsstrecke zur zweiten Datenübertragungseinrichtung ausgelegt werden. In einem solchen System kann beispielsweise ein ausreichend flächendeckendes Netz von zweiten Datenübertragungseinrichtungen realisiert werden, wobei sich eine erste Datenübertragungseinrichtung und eine zweite Datenübertra-

gungseinrichtung dann lediglich ausreichend nahe kommen müssen, um die Übertragung zwischen der mobilen ersten Einrichtung der entfernten Datenzentrale sicherzustellen.

Die vorliegende Erfindung betrifft weiterhin ein Verfahren zur Überwachung einer mobilen ersten Einrichtung, insbesondere eines Fahrzeugs, bei dem zwischen der mobilen ersten Einrichtung und einer von der ersten Einrichtung zumindest zeitweise entfernten Datenzentrale über wenigstens eine mobile erste Übertragungseinrichtung erste Daten mit dem oben beschriebenen erfindungsgemäßen Verfahren übertragen werden. Erfindungsgemäß umfassen die ersten Daten von der ersten Einrichtung zur Datenzentrale übertragene erste Überwachungsdaten. Die ersten Überwachungsdaten umfassen wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße, der von einer ersten Erfassungseinrichtung der ersten Einrichtung erfasst wurde. Diese ersten Überwachungsdaten werden in der Datenzentrale verifiziert. Schließlich werden die ersten Überwachungsdaten bei erfolgreicher Verifikation in der Datenzentrale analysiert.

Vorzugsweise wird in der Datenzentrale in Abhängigkeit von der Analyse der ersten Überwachungsdaten eine erste Überwachungsreaktion ausgelöst. Bei der Überwachungsreaktion kann es sich grundsätzlich um eine beliebige Reaktion handeln.

Bei besonders vorteilhaften Varianten des erfindungsgemäßen Verfahren handelt es sich bei der Überwachungsreaktion um eine Abrechnung handeln. So kann beispielsweise bei der Überwachung der Nutzung von gemieteten oder geleasten mobilen Einheiten, beispielsweise Fahrzeugen, Baumaschinen etc., in Abhängigkeit von der über entsprechende Erfassungseinrichtungen erfassten, übermittelten und analysierten abrechnungsrelevanten Nutzung eine Abrechnung der Nutzung erfolgen. Durch die erfindungsgemäße Authentifizierung der übermittelten Daten ist dabei sichergestellt, dass diese während der Übertragung nicht manipuliert wurden. Erfindungsgemäß ist hierzu vorgesehen, dass die erste Überwachungsreaktion einen Abrechnungsvorgang umfasst.

Zusätzlich oder alternativ können auch beliebige andere Überwachungsreaktionen ausgelöst werden. So können beispielsweise im Rahmen der Überwachung des Betriebszustands von mobilen Einrichtungen so genannte Frühwarnsysteme realisiert werden. Werden beispielsweise über die ersten Daten Fehler oder kritische Zustände bestimmter Einheiten der ersten Einrichtung erfasst oder ergibt sich aus der Analyse der ersten Daten, dass derartige Fehler oder kritische Zustände, gegebenenfalls mit einer bestimmten Wahrscheinlichkeit, innerhalb eines bestimmten Zeitraums eintreten, so kann als Überwachungsreaktion eine entsprechende Mitteilung an die erste Einrichtung übermittelt werden. Die erste Einrichtung kann diese Nachricht dann an den aktuellen Nutzer über eine entsprechend Schnittstelle, bei-

spielsweise optisch und/oder akustisch ausgeben. Es versteht sich, dass diese Nachricht dabei in der oben beschriebenen Weise entsprechend authentifiziert übermittelt werden kann, um Manipulationen auszuschließen. Zusätzlich oder alternativ kann eine solche Nachricht von der Datenzentrale auch automatisch, beispielsweise per Mobilfunk, an einen entsprechend registrierten Nutzer übermittelt werden.

Es versteht sich jedoch, dass nicht nur für die Funktion der mobilen Einheit unmittelbar relevante Erfassungsgrößen erfasst werden können. Mit anderen Worten können beispielsweise auch andere Erfassungsgrößen erfasst werden, welche keinen unmittelbaren Einfluss auf die Funktionsfähigkeit der mobilen Einheit haben.

So kann beispielsweise im Fall von gemieteten oder geleasten mobilen Einheiten die aktuelle Nutzung überwacht werden und als eine Überwachungsreaktion eine entsprechende Nachricht generiert werden, sobald der Nutzer den vereinbarten Nutzungsrahmen überschreitet oder zu überschreiten droht. Ebenso kann bei Überschreiten des vereinbarten Nutzungsrahmens als Überwachungsreaktion auf einen anderen Abrechnungsmodus umgeschaltet werden. War beispielsweise bei einem gemieteten Fahrzeug eine bestimmte Kilometerleistung pauschal vergütet, kann bei Erfassung des Überschreitens dieser Kilometerleistung auf eine kilometerbezogene Abrechnung der Mehrkilometer umgeschaltet werden.

Ebenso kann beispielsweise gemieteten oder geleasten Fahrzeugen oder Maschinen die Position als erste Erfassungsgröße überwacht und analysiert werden. Verstößt der Nutzer gegen eine Vereinbarung, indem das Fahrzeug beispielsweise einen vereinbarten Einsatzbereich verlässt, oder droht ein solcher Verstoß, so kann ebenfalls eine entsprechende Nachricht bzw. Warnung als Überwachungsreaktion übermittelt werden.

Weiterhin kann beispielsweise im Rahmen der Überwachung vorgeschriebener Ruhezeiten für Fahrzeugführer die Betriebsdauer anhand entsprechender Kriterien überwacht werden. Ergibt sich anhand einer oder mehrerer Erfassungsgrößen, dass die vorgeschriebenen Ruhezeiten nicht eingehalten werden bzw. ein Verstoß hiergegen droht, so kann ebenfalls eine entsprechende Nachricht bzw. Warnung als Überwachungsreaktion übermittelt werden.

Der beiden vorgenannten Fällen können im Fall des Verstoßes unter bestimmten Voraussetzungen als weitere Überwachungsreaktion Gegenmaßnahmen eingeleitet werden. Im einfachsten Fall kann dies durch eine entsprechende Mitteilung an eine hoheitliche Einrichtung, wie beispielsweise die Polizei oder dergleichen, übermittelt werden, um den Verstoß abzustellen.

Ebenso kann aber unter Berücksichtigung entsprechender Sicherheitsvorschriften als Überwachungsreaktion einen direkte Beeinflussung der ersten Einrichtung erfolgen. Diese kann gegebenenfalls bis hin zur kontrollierten Abschaltung der ersten Einrichtung reichen.

Eine solche Beeinflussung kann natürlich auch im Fall der oben genannten Überwachung funktionsrelevanter Erfassungsgrößen erfolgen. Vorzugsweise ist daher vorgesehen, dass die erste Überwachungsreaktion die Generierung von Betriebsbeeinflussungsdaten umfasst, die zur Beeinflussung des Betriebs der ersten Einrichtung an die erste Einrichtung übermittelt werden. Wird beispielsweise erfasst, dass für einen bestimmten Betriebsparameter ein kritischer Zustand droht oder vorliegt, können unter Berücksichtigung entsprechender Sicherheitsvorschriften entsprechende Gegenmaßnahmen eingeleitet werden, um diesen kritischen Zustand zu verhindern oder abzustellen. Hierbei ist es unter anderem auch möglich, schadhafte Betriebssoftware oder Teile über eine solche Betriebsbeeinflussung zu warten oder gegebenenfalls sogar vollständig auszutauschen.

In allen vorgenannten Fällen mit entsprechenden Überwachungsreaktionen stellt die Authentifizierung der im Rahmen der Überwachungsreaktion an die mobilen Einheit übermittelten ersten Daten sicher, dass es im Rahmen einer solchen Überwachungsreaktion zu keinen nicht autorisierten Manipulationen kommen kann, sondern lediglich Prozesse ablaufen, die auf entsprechend autorisierten Daten basieren.

Bei weiteren bevorzugten Varianten des erfindungsgemäßen Verfahrens ist vorgesehen, dass bei der Analyse weitere, nicht von der ersten Einrichtung übermittelte Daten berücksichtigt werden. Hierbei kann es sich beispielsweise um statistische Daten handeln, welche durch die Auswertung der Daten gewonnen wurden, die von baugleichen oder ähnlichen ersten Einrichtungen stammen. Ebenso kann es sich aber um, auf anderem Wege zu Datenzentrale gelangte Daten handeln. Insbesondere können bei der Auslösung einer Überwachungsreaktion auch externe Informationen hinsichtlich der ersten Einrichtung berücksichtigt werden. So kann zum Beispiel eine der oben beschriebenen Überwachungsreaktionen ausgelöst werden, wenn in der Datenzentrale eine Information eingeht, dass die erste Einrichtung gestohlen wurde oder dergleichen.

Die vorliegende Erfindung betrifft weiterhin eine Anordnung zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung, insbesondere einem Fahrzeug, und einer von der ersten Einrichtung zumindest zeitweise entfernten Datenzentrale, wobei zur Übertragung der Daten wenigstens eine mobile erste Übertragungseinrichtung vorgesehen ist. Erfindungsgemäß umfassen die übertragenen Daten erste Daten und es ist wenigstens eine Sicherheitseinrichtung vorgesehen, die zum Generieren eines die ersten Daten darstellenden ersten

Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet ist. Die erfindungsgemäße Anordnung eignet sich zur Durchführung des erfindungsgemäßen Verfahrens. Mit ihr lassen sich die vorstehend beschriebenen Ausgestaltungen und Vorteile in derselben Weise realisieren, sodass diesbezüglich auf die obigen Ausführungen verwiesen wird.

Die Sicherheitseinrichtung umfasst dabei ein Kryptographiemodul, welches die oben beschriebenen kryptographischen Mittel zur Verfügung stellt. Die Sicherheitseinrichtung kann dabei insbesondere zur oben beschriebenen Generierung eines MAC ausgebildet sein. Vorzugsweise ist die Sicherheitseinrichtung zur Bildung einer ersten digitalen Signatur unter Verwendung der ersten Daten ausgebildet, um die ersten Daten zu authentifizieren.

Das Kryptographiemodul kann sowohl zur Verschlüsselung zu speichernder Daten verwendet werden als auch zur Verschlüsselung zu übertragender Daten. Es versteht sich, dass je nach Anwendung, also beispielsweise je nachdem, ob Daten versandt oder gespeichert werden sollen, auch unterschiedliche kryptographische Verfahren angewendet werden können.

Neben dem bzw. den kryptographischen Algorithmen und einem oder mehreren entsprechenden kryptographischen Schlüsseln umfassen die Kryptographiedaten das Kryptographiemoduls bevorzugt weitere Daten, wie beispielsweise ein oder mehrere kryptographische Zertifikate entsprechender Zertifizierungsinstanzen sowie gegebenenfalls ein oder mehrere eigene kryptographische Zertifikate der Sicherheitseinrichtung.

Vorzugsweise ist die Sicherheitseinrichtung zum Austausch wenigstens eines Teils der Kryptographiedaten ausgebildet, um in vorteilhafter Weise eine einfache und dauerhaft zuverlässige Sicherung der Daten zu gewährleisten. Hierbei kann insbesondere vorgesehen sein, dass neben den kryptographischen Schlüsseln und kryptographischen Zertifikaten auch der jeweils verwendete kryptographische Algorithmus ausgetauscht werden kann, um das System in einfacher Weise an geänderte Sicherheitsanforderungen anpassen zu können. Die Implementierung und der Austausch der Kryptographiedaten erfolgt bevorzugt im Rahmen einer so genannten Public Key Infrastruktur (PKI), wie sie hinlänglich bekannt ist und daher an dieser Stelle nicht weiter beschrieben werden soll. Es versteht sich insbesondere, dass eine entsprechende Routine zur Überprüfung der Validität der verwendeten kryptographischen Zertifikate vorgesehen ist. Geeignete derartige Überprüfungsroutinen sind ebenfalls hinlänglich bekannt und sollen daher hier nicht näher beschrieben werden

Vorzugsweise ist die Sicherheitseinrichtung zur oben beschriebenen Authentifizierung einer ersten Quelle der ersten Daten ausgebildet. Hierzu ist die Sicherheitseinrichtung bevorzugt

zum Einbringen einer ersten Quellenidentifikation in den ersten Datensatz ausgebildet. Weiter vorzugsweise ist die Sicherheitseinrichtung zur oben beschriebenen Authentifizierung eines ersten Empfängers der ersten Daten ausgebildet. Hierzu ist sie vorzugsweise zum Einbringen einer ersten Empfängeridentifikation in den ersten Datensatz ausgebildet.

Bei bevorzugten Varianten der erfindungsgemäßen Anordnung ist die Sicherheitseinrichtung zur Authentifizierung der Übertragung der ersten Daten ausgebildet. Hierzu ist sie bevorzugten zum Einbringen einer Übertragungsidentifikation in den ersten Datensatz ausgebildet. Weiterhin ist die Sicherheitseinrichtung vorzugsweise zum Einbringen wenigstens einer für ein vorgebbares Ereignis charakteristischen Zeitkennung in den ersten Datensatz ausgebildet.

Bei weiteren vorteilhaften Varianten der erfindungsgemäßen Anordnung ist vorgesehen, dass die Sicherheitseinrichtung zum Einbringen der authentifizierten ersten Daten in einen Protokolldatensatz ausgebildet ist. Die erste Einrichtung weist dann einen ersten Protokollspeicher zum Speichern des Protokolldatensatzes auf. Zusätzlich oder alternativ weist die Datenzentrale einen zweiten Protokollspeicher zum Speichern des Protokolldatensatzes auf.

Die Sicherheitseinrichtung kann grundsätzlich an beliebiger Stelle in der Übertragungsstrecke angeordnet sein. Bevorzugt umfasst die erste Einrichtung eine erste derartige Sicherheitseinrichtung. Zusätzlich oder alternativ umfasst die Datenzentrale eine zweite derartige Sicherheitseinrichtung.

Bei vorteilhaften Varianten der erfindungsgemäßen Anordnung umfassen die ersten Daten von der ersten Einrichtung zur Datenzentrale übertragene erste Überwachungsdaten. Diese Überwachungsdaten umfassen wiederum wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße. Die erste Einrichtung umfasst weiterhin eine erste Erfassungseinrichtung zur Erfassung des ersten Erfassungswerts. Bei den Erfassungsgrößen kann es sich, wie oben erwähnt, um beliebige erfassbare Größen handeln. Bevorzugt ist die erste Erfassungseinrichtung zur Erfassung einer Zustandsgröße der ersten Einrichtung als erster Erfassungsgröße ausgebildet.

Bei weiteren bevorzugten Varianten der erfindungsgemäßen Anordnung ist vorgesehen, dass die ersten Daten von der Datenzentrale zur ersten Einrichtung übertragene Betriebsbeeinflussungsdaten umfassen. Die erste Einrichtung umfasst dann eine Betriebsbeeinflussungseinrichtung, um hierüber den Betrieb der ersten Einrichtung in Abhängigkeit von den Betriebsbeeinflussungsdaten zu beeinflussen, wie dies oben im Zusammenhang mit dem erfindungsgemäßen Verfahren beschrieben wurde.

Die vorliegende Erfindung betrifft weiterhin eine Anordnung zur Überwachung einer mobilen ersten Einrichtung, insbesondere eines Fahrzeugs, mit einer erfindungsgemäßen Anordnung zur Übertragung von ersten Daten. Die ersten Daten umfassen dabei von der ersten Einrichtung zur Datenzentrale übertragene erste Überwachungsdaten, die wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße umfassen. Die erste Einrichtung umfasst weiterhin eine erste Erfassungseinrichtung zur Erfassung des ersten Erfassungswerts. Die Datenzentrale weist eine zweite Sicherheitseinrichtung zum Verifizieren der ersten Überwachungsdaten auf. Weiterhin weist die Datenzentrale eine mit der zweiten Sicherheitseinrichtung verbundene Analyseeinrichtung zum Analysieren der ersten Überwachungsdaten in Abhängigkeit vom Ergebnis der Verifikation auf. Diese erfindungsgemäße Anordnung eignet sich zur Durchführung des erfindungsgemäßen Verfahrens zur Überwachung einer mobilen ersten Einrichtung. Mit ihr lassen sich die vorstehend beschriebenen Ausgestaltungen und Vorteile in derselben Weise realisieren, sodass diesbezüglich auf die obigen Ausführungen verwiesen wird.

Bevorzugt ist wenigstens eine mit der Analyseeinrichtung verbindbare Überwachungsreaktionseinrichtung zur Durchführung einer ersten Überwachungsreaktion vorgesehen. Die Analyseeinrichtung ist dann zum Ansteuern der Überwachungsreaktionseinrichtung ausgebildet, um eine erste Überwachungsreaktion in Abhängigkeit vom Ergebnis der Analyse der ersten Überwachungsdaten auszulösen.

Vorzugsweise ist als Überwachungsreaktionseinrichtung eine mit der Analyseeinrichtung verbindbare Abrechnungseinrichtung vorgesehen. Weiter vorzugsweise ist die Überwachungsreaktionseinrichtung zur Generierung von Betriebsbeeinflussungsdaten als erste Überwachungsreaktion ausgebildet, wobei Betriebsbeeinflussungsdaten die zur Beeinflussung des Betriebs der ersten Einrichtung dienen. Die Datenzentrale ist dann zur Übertragung erster Daten an die erste Einrichtung ausgebildet, wobei die ersten Daten die Betriebsbeeinflussungsdaten umfassen. Schließlich weist die erste Einrichtung eine Betriebsbeeinflussungseinrichtung zur Beeinflussung des Betriebs der ersten Einrichtung in Abhängigkeit von den Betriebsbeeinflussungsdaten auf.

Bei weiteren bevorzugten Varianten der erfindungsgemäßen Anordnung umfasst die erste Einrichtung eine erste Sicherheitseinrichtung, die zum Verifizieren der die Betriebsbeeinflussungsdaten umfassenden ersten Daten ausgebildet ist. Die Betriebsbeeinflussungseinrichtung ist dann zur Beeinflussung des Betriebs der ersten Einrichtung in Abhängigkeit vom Ergebnis der Verifizierung ausgebildet.

Die vorliegende Erfindung betrifft weiterhin eine mobile erste Einrichtung, insbesondere Fahrzeug, für eine erfindungsgemäße Anordnung. Erfindungsgemäß umfasst die erste Einrichtung eine erste Datenübertragungseinrichtung zur Übertragung erster Daten und eine mit der ersten Datenübertragungseinrichtung verbindbare erste Sicherheitseinrichtung. Die Sicherheitseinrichtung ist zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet.

Bei einer bevorzugten Ausgestaltung der erfindungsgemäßen mobilen Einrichtung ist die erste Sicherheitseinrichtung zur Authentifizierung der ersten Datenübertragungseinrichtung ausgebildet. Hierzu ist sie bevorzugt zum Einbringen einer der ersten Datenübertragungseinrichtung zugeordneten Identifikation in den ersten Datensatz ausgebildet.

Die vorliegende Erfindung betrifft schließlich eine Datenzentrale für eine erfindungsgemäße Anordnung. Erfindungsgemäß weist die Datenzentrale eine Datenübertragungseinrichtung zur Übertragung erster Daten und eine mit der Datenübertragungseinrichtung verbindbare zweite Sicherheitseinrichtung auf, die zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet ist.

Um erhöhten Schutz vor unerkannter unbefugter Manipulation der gespeicherten ersten Daten, insbesondere der gespeicherten Erfassungswerte zu erzielen, ist die jeweilige Sicherheitseinrichtung bevorzugt zur Überprüfung der Zugriffsberechtigung auf wenigstens einen Teil der Sicherheitseinrichtung oder anderer Teile der ersten Einrichtung bzw. der Datenzentrale ausgebildet. Die Überprüfung kann sich dabei auf einzelne, entsprechend sicherheitsrelevante Bereiche der Sicherheitseinrichtung beschränken. Sie kann sich jedoch auch auf die Überprüfung der Zugriffsberechtigung für sämtliche Bereiche der Sicherheitseinrichtung erstrecken.

Bevorzugt wird schon die Zugriffsberechtigung auf den Speicher überprüft, in dem die ersten Daten gespeichert sind, um den unberechtigten Zugriff auf die ersten Daten zu verhindern. Es versteht sich jedoch, dass bei bestimmten Varianten der erfindungsgemäßen Anordnung der Zugriff auf den Speicher für die ersten Daten auch ohne besondere Zugriffsberechtigung zugelassen sein kann, wenn die ersten Daten bereits in entsprechend authentifizierter Weise gespeichert sind, dass nicht autorisierte Manipulationen an den ersten Daten erkennbar sind. Dies ist der Fall, wenn die ersten Daten beispielsweise bereits zusammen mit einer unter Verwendung der ersten Daten erzeugten Authentifizierungsinformation, wie beispielsweise einem obengenannten MAC, einer digitalen Signatur oder dergleichen gespeichert sind. Die Authentifizierungsinformation wird dann bevorzugt, in einem Bereich der Sicherheitseinrich-

tung erzeugt, für den die Zugriffsberechtigung, sofern der Zugriff überhaupt möglich ist, überprüft wird.

Hierdurch wird erreicht, dass eine unbefugte Manipulation des gespeicherten ersten Daten zum einen entweder mangels Zugriff auf die ersten Daten überhaupt nicht möglich ist oder bei einer Überprüfung zumindest nicht unerkannt bleibt.

Die Überprüfung der Zugriffsberechtigung kann grundsätzlich in beliebiger geeigneter Weise erfolgen. So ist es beispielsweise möglich, ein Passwortsystem oder dergleichen zu implementieren. Bevorzugt ist vorgesehen, dass die Verarbeitungseinheit zur Überprüfung der Zugriffsberechtigung unter Einsatz kryptographischer Mittel ausgebildet ist. Hierbei können beispielsweise digitale Signaturen und kryptographische Zertifikate zur Anwendung kommen. Dies ist von besonderem Vorteil, da derartige kryptographische Verfahren einen besonders hohen Sicherheitsstandard gewährleisten.

Hierbei können im übrigen wenigstens zwei unterschiedliche Zugriffsberechtigungsstufen vorgesehen sein, die mit unterschiedlichen Zugriffsrechten auf die Sicherheitseinrichtung bzw. mit ihr verbundenen Einrichtungen verknüpft sind. Hiermit lässt sich in einfacher Weise zum einen eine hierarchische Struktur mit unterschiedlich weit gehenden Zugriffsrechten implementieren. So kann beispielsweise dem Benutzer der Anordnung auf der untersten Zugriffsberechtigungsstufe als einzige Zugriffshandlung erlaubt sein, die gespeicherten ersten Daten auszulesen, während einem Administrator auf einer höheren Zugriffsberechtigungsstufe neben dem Auslesen der ersten Daten gegebenenfalls die Modifikation weiterer Komponenten der Sicherheitseinrichtung etc. möglich ist.

Zum anderen lässt sich über die Zugriffsberechtigungsstufen auf derselben Hierarchieebene aber auch der Zugriff auf unterschiedliche Bereiche der Sicherheitseinrichtung bzw. mit ihr verbundenen Einrichtungen steuern. Die Anzahl der Zugriffsberechtigungsstufen oder Klassen richtet sich dabei nach der jeweiligen Verwendung der Anordnung und der Komplexität der mit der erfindungsgemäßen Anordnung realisierbaren Anwendungen.

Bei bevorzugten Ausgestaltungen der erfindungsgemäßen Anordnung werden die ersten Erfassungswerte verknüpft mit einer für den Erfassungszeitpunkt des ersten Erfassungswerts charakteristischen Erfassungszeitkennung ausgebildet. Durch diese häufig auch als Zeitstempel bezeichnete Verknüpfung des gespeicherten ersten Erfassungswerts mit dem Zeitpunkt seiner Erfassung wird die Weiterverarbeitung des Erfassungswerts, beispielsweise zu Zwecken der Abrechnung aber auch zu Zwecken der Statistik etc. deutlich erleichtert.

Dies gilt insbesondere dann, wenn mehrere, zu unterschiedlichen Zeiten erfasste erste Erfassungswerte verarbeitet werden sollen.

Es versteht sich jedoch, dass es bei anderen Varianten der Erfindung ohne derartige Zeitstempel auch ausreichen kann, wenn lediglich durch geeignete Maßnahmen sichergestellt ist, dass die Chronologie der Erfassung der ersten Erfassungswerte nachvollziehbar ist. So können den ersten Erfassungswerten beispielsweise fortlaufende Nummern zugeordnet werden, um dieses Ziel zu erreichen.

Die Ermittlung der Erfassungszeit kann auf beliebige geeignete Weise erfolgen. Bevorzugt umfasst die Sicherheitseinrichtung zur Ermittlung der Erfassungszeitkennung ein mit der Verarbeitungseinheit verbundenes Zeiterfassungsmodul. Hierbei kann es sich um eine integrierte Echtzeituhr handeln oder ein Modul, das über eine geeignete Kommunikationsverbindung zu einer entsprechenden Instanz die Echtzeit abfragt. Die integrierte Echtzeituhr kann dabei gegebenenfalls von Zeit zu Zeit mit einer entsprechend genauen Zeitquelle synchronisiert werden.

Bei besonders günstigen Varianten der Erfindung ist wenigstens eine zweite Erfassungseinrichtung zur Erfassung wenigstens eines zweiten Erfassungswerts der ersten Erfassungsgröße vorgesehen. Mit diesen Varianten ist es möglich, auch größere Systeme mit mehreren Erfassungsorten der Erfassungsgröße, beispielsweise mehreren Messstellen für den Verbrauch eines Verbrauchsgutes, mit einer reduzierten Anzahl von Sicherheitseinrichtungen, gegebenenfalls sogar mit einer einzigen Sicherheitseinrichtung zu betreiben. Um die Trennung der ersten und zweiten Erfassungswerte sicherzustellen, kann vorgesehen sein, dass die ersten und zweiten Erfassungswerte in unterschiedlichen Speicherbereichen abgelegt werden. Hierbei können insbesondere unterschiedliche Zugriffsberechtigungen für die unterschiedlichen Speicherbereiche definiert sein, um sicherzustellen, dass nur die jeweils autorisierten Personen bzw. Einrichtungen auf den entsprechenden Speicherbereich zugreifen können.

Besonders vorteilhaft ist es jedoch, wenn der erste Erfassungswert verknüpft mit einer für die erste Erfassungseinrichtung charakteristischen ersten Erfassungseinrichtungskennung und der zweite Erfassungswert verknüpft mit einer für die zweite Erfassungseinrichtung charakteristischen zweiten Erfassungseinrichtungskennung gespeichert wird. Mit dieser eindeutigen Zuordnung zwischen der Erfassungseinrichtung und dem durch sie erfassten Erfassungswerts ist eine besonders einfache und zuverlässige Trennung möglich, welche die spätere Weiterverarbeitung erheblich erleichtert.

Bei weiteren günstigen Ausgestaltungen der erfindungsgemäßen Anordnung ist vorgesehen, dass die erste Erfassungseinrichtung zur Erfassung wenigstens eines dritten Erfassungswerts einer zweiten Erfassungsgröße ausgebildet ist. Alternativ kann eine dritte Erfassungseinrichtung zur Erfassung wenigstens eines dritten Erfassungswerts einer zweiten Erfassungsgröße vorgesehen sein. Hierdurch ist es möglich, mit einer einzigen Sicherheitseinrichtung die Erfassung und gesicherte Speicherung der Erfassungswerte für unterschiedliche Erfassungsgrößen zu realisieren.

Um die Trennung der ersten und dritten Erfassungswerte sicherzustellen, kann auch hier wieder vorgesehen sein, dass die ersten und dritten Erfassungswerte in unterschiedlichen Speicherbereichen abgelegt werden. Besonders vorteilhaft ist es jedoch auch hier, wenn der erste Erfassungswert verknüpft mit einer für die erste Erfassungsgröße charakteristischen ersten Erfassungsgrößenkennung und der dritte Erfassungswert verknüpft mit einer für die zweite Erfassungsgröße charakteristischen zweiten Erfassungsgrößenkennung gespeichert wird. Mit dieser eindeutigen Zuordnung zwischen der Erfassungseinrichtung und der durch sie erfassten Erfassungsgröße ist eine besonders einfache und zuverlässige Trennung möglich, welche die spätere Weiterverarbeitung der gespeicherten Daten erheblich erleichtert.

Bei bevorzugten Varianten der erfindungsgemäßen Anordnung sind die erste Erfassungseinrichtung und die Sicherheitseinrichtung in einer vor unbefugtem Zugriff geschützten sicheren Umgebung angeordnet, um in vorteilhafter Weise den unbefugten Zugriff nicht nur auf die Daten der Sicherheitseinrichtung sondern auch auf die Daten, die von und zu der ersten Erfassungseinrichtung geliefert werden, wirksam zu unterbinden.

Die sichere Umgebung kann dabei physisch durch ein oder mehrere entsprechend gesicherte Gehäuse hergestellt werden. Diese Gehäuse sind dann bevorzugt mit entsprechenden, hinlänglich bekannten Mitteln zur Erfassung von Manipulationen am Gehäuse ausgestattet. Bevorzugt erfolgt die Sicherung jedoch auch logisch durch ein entsprechend abgesichertes Kommunikationsprotokoll zwischen der ersten Erfassungseinrichtung und der Sicherheitseinrichtung. So kann beispielsweise vorgesehen sein, dass bei jeder Kommunikation zwischen der ersten Erfassungseinrichtung und der Sicherheitseinrichtung über eine entsprechend starke gegenseitige Authentifizierung ein gesicherter Kommunikationskanal aufgebaut wird. Es versteht sich, dass die erste Erfassungseinrichtung in diesem Fall über entsprechende Kommunikationsmittel verfügt, welche die beschriebene Sicherheitsfunktionalität zur Verfügung stellen.

Es versteht sich weiterhin, dass die sichere Umgebung durch solche logischen Sicherungsmechanismen auf einen beliebig großen Raum erstreckt werden kann. So können die erste

Erfassungseinrichtung und die Sicherheitseinrichtung bei solchen Ausführungen innerhalb der sicheren Umgebung weit voneinander entfernt angeordnet sein. Es versteht sich weiterhin, dass die sichere Umgebung durch solche logischen Sicherungsmechanismen auch auf andere Komponenten, beispielsweise das Datenzentrum, ausgeweitet werden kann.

Es versteht sich, dass sämtliche der oben beschriebenen Module und Funktionen der Sicherheitseinrichtung durch entsprechend gestaltete Hardwaremodule realisiert sein können. Bevorzugt sind sie jedoch zumindest zum Teil als Softwaremodule gestaltet, auf welche die Verarbeitungseinheit zugreift, um die entsprechende Funktion zu realisieren. Weiterhin versteht es sich, dass die einzelnen Speicher nicht durch getrennte Speichermodule realisiert sein müssen. Vielmehr handelt es sich bevorzugt um entsprechend logisch getrennte Speicherbereiche eines einzigen Speichers, beispielsweise eines einzigen Speichermoduls.

Weitere bevorzugte Ausgestaltungen der Erfindung ergeben sich aus den Unteransprüchen bzw. der nachstehenden Beschreibung eines bevorzugten Ausführungsbeispiels, welche auf die beigefügten Zeichnungen Bezug nimmt. Es zeigen

Figur 1 eine schematische Darstellung einer bevorzugten Ausführungsform der erfindungsgemäßen Anordnung zur Durchführung des erfindungsgemäßen Verfahrens;

Figur 2 ein Blockschaltbild von Komponenten der Anordnung aus Figur 1;

Figur 3 eine schematische Darstellung einer weiteren bevorzugten Ausführungsform der erfindungsgemäßen Anordnung;

Figur 4 eine schematische Darstellung einer weiteren bevorzugten Ausführungsform der erfindungsgemäßen Anordnung.

Figur 1 zeigt ein bevorzugtes Ausführungsbeispiel der erfindungsgemäßen Anordnung zur Durchführung des erfindungsgemäßen Verfahrens zur Übertragung von Daten zwischen einer mobilen ersten Einrichtung in Form eines Fahrzeugs 1 und einer davon entfernten Datenzentrale 2. Bei dem Fahrzeug 1 handelt es sich im vorliegenden Beispiel um einen Mietwagen. Die vorliegende Erfindung wird hierbei im Zusammenhang mit der Überwachung und insbesondere mit der Abrechnung für die Nutzung dieses Mietwagens eingesetzt.

Das Fahrzeug 1 umfasst eine mobile erste Übertragungseinrichtung in Form eines ersten Mobilfunkmoduls 1.1 für ein Mobilfunknetz 3. Mittels des Mobilfunkmoduls 1.1 können Daten

über eine zweite Übertragungseinrichtung 3.1 des Mobilfunknetzes 3 mit einer dritten Übertragungseinrichtung in Form eines zweiten Mobilfunkmoduls 2.1 der Datenzentrale 2 ausgetauscht werden.

Das Fahrzeug 1 weist weiterhin eine mit dem ersten Mobilfunkmodul 1.1 verbundene erste Sicherheitseinrichtung in Form eines ersten Sicherheitsmoduls 1.2 auf. Spätestens wenn über das Mobilfunknetz 3 sicherheitsrelevante Daten von dem Fahrzeug 1 zur Datenzentrale 2 übertragen werden sollen, generiert das erste Sicherheitsmodul 1.2 einen erste Daten darstellenden ersten Datensatz, der unter anderem die zu übertragenden sicherheitsrelevanten Daten umfasst. Anschließend authentifiziert das erste Sicherheitsmodul 1.2 die ersten Daten unter Verwendung kryptographischer Mittel.

Hierzu ordnet das erste Sicherheitsmodul 1.2 dem ersten Datensatz eine Authentifizierungsinformation zu, indem es zunächst unter Verwendung eines entsprechenden kryptographischen Algorithmus und eines privaten ersten kryptographischen Schlüssels des Sicherheitsmoduls 1.2 über dem ersten Datensatz eine erste digitale Signatur als Authentifizierungsinformation bildet. Anschließend bildet das Sicherheitsmodul 1.2 aus dem ersten Datensatz und der ersten digitalen Signatur einen zweiten Datensatz.

Die erste digitale Signatur, also die Authentifizierungsinformation, stellt sicher, dass zu einem späteren Zeitpunkt durch eine Verifikation der ersten digitalen Signatur zweifelsfrei festgestellt werden kann, ob der erste Datensatz und damit die ersten Daten manipuliert wurden oder ob es sich nach wie vor um authentische Daten handelt.

Um die Sicherheit vor unbefugtem Zugriff auf die Daten zu erhöhen, verschlüsselt das erste Sicherheitsmodul 1.2 den zweiten Datensatz unter Verwendung eines zweiten kryptographischen Schlüssels, wobei ein dritter Datensatz entsteht. Dieser dritte Datensatz wird von dem ersten Sicherheitsmodul 1.2 an das erste Mobilfunkmodul 1.1 übergeben. Das erste Mobilfunkmodul 1.1 überträgt den dritten Datensatz dann über das Mobilfunknetz 3 an das zweite Mobilfunkmodul 2.1 der Datenzentrale 2.

Das zweite Mobilfunkmodul 2.1 gibt den dritten Datensatz an eine damit verbundene zweite Sicherheitseinrichtung in Form eines zweiten Sicherheitsmoduls 2.2 weiter. Das zweite Sicherheitsmodul 2.2 entschlüsselt den und dritten Datensatz unter Verwendung eines dritten kryptographischen Schlüssels, um so wieder den zweiten Datensatz zu erhalten. Der dritte Schlüssel entspricht dabei dem zweiten Schlüssel. Es handelt sich hierbei im vorliegenden Fall um einen zuvor ausschließlich für diese Übertragungssitzung generierten geheimen Sitzungsschlüssel. Dieser wurde zuvor separat in dem ersten Sicherheitsmodul 1.2 und dem

zweiten Sicherheitsmodul 2.2 generiert. Die Generierung und Verwendung solcher geheimer einmalig verwendeter Sitzungsschlüssel ist an sich bekannt, sodass hierauf an dieser Stelle nicht näher eingegangen werden soll.

Es versteht sich jedoch, dass bei anderen Varianten der Erfindung, sofern eine solche Absicherung erforderlich ist, auch ein anderer Absicherungsmechanismus gewählt werden kann. Insbesondere kann bei Verwendung einer asymmetrischen Verschlüsselung der zweite kryptographische Schlüssel beispielsweise ein öffentlicher Schlüssel des zweiten Sicherheitsmoduls sein. Der dritte Schlüssel ist dann entsprechend der zugehörige private Schlüssel des zweiten Sicherheitsmoduls.

Aus dem zweiten Datensatz extrahiert das zweite Sicherheitsmodul 2.2 den ersten Datensatz und die erste digitale Signatur. Anhand des ersten Datensatzes und eines dem ersten kryptographischen Schlüssel zugeordneten vierten kryptographischen Schlüssels verifiziert das zweite Sicherheitsmodul 2.2 dann in an sich bekannter Weise die erste digitale Signatur, um die Authentizität des ersten Datensatzes und damit der ersten Daten festzustellen.

Derselbe Ablauf ergibt sich in der anderen Richtung, wenn sicherheitsrelevante Daten von der Datenzentrale 2 an das Fahrzeug 1 übermittelt werden sollen. Hierbei führt das zweite Sicherheitsmodul 2.2 dann die oben für das erste Sicherheitsmodul 1.2 beschriebenen Operationen durch und umgekehrt.

Im Rahmen der Kommunikation zwischen dem Fahrzeug 1 und der Datenzentrale 2 findet eine starke wechselseitige Authentifizierung der Kommunikationspartner unter Einsatz entsprechender kryptographischer Mittel statt, wobei insbesondere entsprechende kryptographische Zertifikate Verwendung finden. Dies geschieht wiederum unter Verwendung des ersten Sicherheitsmoduls 1.2 und des zweiten Sicherheitsmoduls 2.2. Verfahren für eine solche starke wechselseitige Authentifizierung der Kommunikationspartner sind hinlänglich bekannt, sodass hierauf nicht näher eingegangen werden soll.

Figur 2 zeigt ein Blockschaltbild von Komponenten des Fahrzeugs 1. Wie dieser Figur zu entnehmen ist, weist das erste Sicherheitsmodul 1.2 eine erste Verarbeitungseinheit 1.3 auf, die mit dem ersten Mobilfunkmodul 1.1 verbunden ist. Mit der ersten Verarbeitungseinheit 1.3 ist weiterhin ein Kryptographiemodul 1.4 verbunden, welches die oben beschriebenen kryptographischen Mittel zur Verfügung stellt und hierzu entsprechende Kryptographiedaten enthält. Die Kryptographiedaten umfassen unter anderem kryptographischen Algorithmen und entsprechende kryptographische Schlüssel. Neben den kryptographischen Algorithmen und Schlüsseln umfassen die Kryptographiedaten des Kryptographiemoduls 1.4 weitere Da-

ten, wie beispielsweise ein oder mehrere kryptographische Zertifikate entsprechender Zertifizierungsinstanzen sowie gegebenenfalls ein oder mehrere eigene kryptographische Zertifikate der Sicherheitseinrichtung 1.2.

Das Sicherheitsmodul 1.2 ist zum Austausch wenigstens eines Teils der Kryptographiedaten ausgebildet, um eine einfache und dauerhaft zuverlässige Sicherung der Daten zu gewährleisten. Hierbei ist vorgesehen, dass neben den kryptographischen Schlüsseln und kryptographischen Zertifikaten auch der jeweils verwendete kryptographische Algorithmus ausgetauscht werden kann, um das System an geänderte Sicherheitsanforderungen anpassen zu können. Die Implementierung und der Austausch der Kryptographiedaten erfolgt im Rahmen einer so genannten Public Key Infrastruktur (PKI), wie sie hinlänglich bekannt ist und daher an dieser Stelle nicht weiter beschrieben werden soll. Es versteht sich insbesondere, dass eine entsprechende Routine zur Überprüfung der Validität der verwendeten kryptographischen Zertifikate vorgesehen ist. Geeignete derartige Überprüfungsroutinen sind ebenfalls hinlänglich bekannt und sollen daher hier nicht näher beschrieben werden

Das Kryptographiemodul 1.4 wird sowohl zur Verschlüsselung zu speichernder Daten verwendet werden als auch zur Verschlüsselung zu übertragender Daten. Es versteht sich, dass je nach Anwendung, also beispielsweise je nachdem, ob Daten versandt oder gespeichert werden sollen, auch unterschiedliche kryptographische Verfahren angewendet werden können.

Nach der erfolgreichen Übertragung des dritten Datensatzes erstellt das erste Sicherheitsmodul 1.2 einen Protokolldatensatz, den es in einem mit der ersten Verarbeitungseinheit 1.3 verbundenen ersten Protokollspeicher 1.5 ablegt. Der Protokolldatensatz umfasst den ersten Datensatz sowie die über dem ersten Datensatz in der oben beschriebenen Weise erstellte erste digitale Signatur. Der umfasst mit anderen Worten also die authentifizierten ersten Daten. Der erste Protokollspeicher 1.5 kann dabei so gestaltet sein, dass der Protokolldatensatz lediglich gelesen aber nicht verändert werden kann. Weiterhin kann der erste Protokollspeicher 1.5 so dimensioniert sein, dass er sämtliche über die Lebensdauer des ersten Sicherheitsmoduls 1.2 oder des Fahrzeugs 1 zu erwartenden Protokolldatensätze aufnehmen kann.

Im vorliegenden Beispiel werden die Protokolldatensätze im Klartext gespeichert. Es versteht sich jedoch, dass bei anderen Varianten der Erfindung vorgesehen sein kann, dass die Protokolldatensätze in verschlüsselter Form gespeichert werden können, um sie vor unbefugter Einsicht zu schützen.

Im Folgenden wird unter Bezugnahme auf die Figuren 1 und 2 die Generierung der an die Datenzentrale 2 zu übertragenden sicherheitsrelevanten ersten Daten näher beschrieben.

Die ersten Daten umfassen zum einen erste Erfassungswerte einer ersten Erfassungsgröße, die durch eine mit der ersten Verarbeitungseinheit 1.3 verbundene erste Erfassungseinrichtung 4 erfasst wurden. Bei den ersten Erfassungswerten handelt es sich um die aktuellen Werte des Kilometerstands des Fahrzeugs 1 als erster Erfassungsgröße. Diese Kilometerwerte werden von dem Kilometerzähler 4 des Fahrzeugs 1 als erster Erfassungseinrichtung erfasst und zu vorgegebenen Zeiten, beispielsweise in regelmäßigen Abständen, an die erste Verarbeitungseinheit 1.3 weitergegeben.

Die erste Verarbeitungseinheit 1.3 verknüpft diese Kilometerwerte mit einer für den Zeitpunkt ihrer Erfassung charakteristischen Erfassungszeitkennung, einem so genannten Zeitstempel, indem sie den Kilometerwert und die Erfassungszeitkennung in einen ersten Kilometerdatensatz schreibt. Hierzu greift sie auf ein Zeiterfassungsmodul 1.6 des ersten Sicherheitsmoduls 1.2 zu, welches eine entsprechend zuverlässige Zeitinformation liefert. Bei dem Zeiterfassungsmodul handelt es sich um eine integrierte Echtzeituhr, die von Zeit zu Zeit mit einer entsprechend genauen Zeitquelle synchronisiert wird. Es versteht sich, dass es sich bei anderen Varianten der Erfindung ebenso um ein Modul handeln kann, das über eine geeignete Kommunikationsverbindung zu einer entsprechenden Instanz die Echtzeit abfragt.

Die erste Verarbeitungseinheit 1.3 verknüpft die Kilometerwerte weiterhin mit einer für den Kilometerzähler 4 charakteristischen ersten Erfassungseinrichtungskennung, indem sie diese ebenfalls in den ersten Kilometerdatensatz schreibt. Hierbei handelt es sich um eine für den betreffenden Kilometerzähler 4 einmalige und eindeutige Identifikation, die gleichzeitig eine erste Quellenidentifikation für die Quelle der Kilometerwerte darstellt. Die erste Erfassungseinrichtungskennung stellt gleichzeitig eine erste Erfassungsgrößenkennung dar, da der Kilometerzähler 4 ausschließlich Kilometerwerte liefert. Es versteht sich, dass bei anderen Erfassungseinrichtungen, die unterschiedliche Erfassungsgrößen erfassen, den jeweiligen Erfassungswerten gegebenenfalls mit einer entsprechenden Erfassungsgrößenkennung verknüpft werden können.

Es versteht sich, dass die vorgenannte Verknüpfung der Kilometerwerte mit der Erfassungszeitkennung und der Erfassungseinrichtungskennung durch kryptographische Mittel abgesichert werden kann. So kann beispielsweise vorgesehen sein, dass das erste Sicherheitsmodul 1.2 eine zweite digitale Signatur über diesen Daten erstellt, sodass diese durch die ihnen dann beigefügte zweite digitale Signatur ebenfalls manipulationssichere miteinander ver-

knüpft sind. Ebenso kann natürlich für beliebige andere einander zugeordnete Daten verfahren werden, um diese manipulationssicher miteinander zu verknüpfen.

Der so generierte erste Kilometerdatensatz wird dann von der ersten Verarbeitungseinheit 1.3 in einem mit ihr verbundenen ersten Speicher 1.7 abgelegt.

Die ersten Daten umfassen weiterhin zweite Erfassungswerte einer zweiten Erfassungsgröße und dritte Erfassungswerte einer dritten Erfassungsgröße, die durch eine mit der ersten Verarbeitungseinheit 1.3 verbundene zweite Erfassungseinrichtung 5 erfasst wurden. Bei den zweiten Erfassungswerten handelt es sich um die aktuellen Werte des Motorölstands des Fahrzeugs 1 als zweiter Erfassungsgröße. Bei dritten Erfassungswerten handelt es sich um die aktuellen Werte der Bremsenqualität des Fahrzeugs 1 als dritter Erfassungsgröße. Diese Bremsenqualitätswerte werden von der Fahrzeugüberwachungseinrichtung 5 des Fahrzeugs 1 als zweiter Erfassungseinrichtung erfasst und ebenfalls zu vorgegebenen Zeiten, beispielsweise in regelmäßigen Abständen, an die erste Verarbeitungseinheit 1.3 weitergegeben.

Die erste Verarbeitungseinheit 1.3 verknüpft diese zweiten und dritten Erfassungswerte mit einer für den Zeitpunkt ihrer Erfassung charakteristischen Erfassungszeitkennung, indem sie den Motorölstandswert, den Bremsenqualitätswert und die Erfassungszeitkennung in einen ersten Fahrzeugzustandsdatensatz schreibt. Hierzu greift sie auf ein Zeiterfassungsmodul 1.6 der ersten Sicherheitseinrichtung 1.2 zu.

Die erste Verarbeitungseinheit 1.3 verknüpft die Motorölstandswerte und die Bremsenqualitätswerte weiterhin mit einer für die Fahrzeugüberwachungseinrichtung 5 charakteristischen zweiten Erfassungseinrichtungskennung, indem sie diese ebenfalls in den ersten Fahrzeugzustandsdatensatz schreibt. Hierbei handelt es sich um eine für die betreffende Fahrzeugüberwachungseinrichtung 5 einmalige und eindeutige Identifikation, die gleichzeitig eine zweite Quellenidentifikation für die Quelle der Motorölstandswerte und Bremsenqualitätswerte darstellt. Weiterhin wird den jeweiligen Erfassungswerten eine entsprechenden Erfassungsgrößenkennung zugeordnet, indem diese entsprechend zugeordnet mit in den Fahrzeugzustandsdatensatz geschrieben wird.

Der so generierte erste Fahrzeugzustandsdatensatz wird dann von der ersten Verarbeitungseinheit 1.3 ebenfalls in dem ersten Speicher 1.7 abgelegt.

Zu einem bestimmten vorgegebenen oder wählbaren Zeitpunkt sollen dann die zwischenzeitlich im ersten Speicher 1.7 abgelegten Kilometerdatensätze und Fahrzeugzustandsdatensät-

ze als erste Überwachungsdaten an die Datenzentrale 2 übertragen werden. Die erste Verarbeitungseinheit 1.3 liest hierzu die gespeicherten Kilometerdatensätze und Fahrzeugzustandsdatensätze aus dem ersten Speicher 1.7 aus und schreibt sie in den ersten Datensatz.

Die erste Verarbeitungseinheit 1.3 ergänzt den ersten Datensatz weiterhin um eine dem ersten Sicherheitsmodul 1.2 zugeordnete einmalige und eindeutige erste Sicherheitsmodulidentifikation sowie um einen unter Zugriff auf das erste Zeiterfassungsmodul 1.6 generierten ersten Zeitstempel. Die erste Sicherheitsmodulidentifikation stellt dabei eine dritte Quellenidentifikation dar, während der erste Zeitstempel den Zeitpunkt der Zusammenstellung der erste Überwachungsdaten charakterisiert. Weiterhin ergänzt die erste Verarbeitungseinheit 1.3 den ersten Datensatz um eine einmalige und eindeutige Identifikation des ersten Mobilfunkmoduls 1.1, die ebenfalls als Quellenidentifikation dient.

Schließlich ergänzt die erste Verarbeitung einer 1.3 den ersten Datensatz um eine Übertragungsidentifikation in Form einer fortlaufenden Transaktionsnummer, die dem laufenden Übertragungsvorgang eindeutig zugeordnet ist.

Anschließend wird der erste Datensatz in der oben beschriebenen Weise authentifiziert und in Form des dritten Datensatzes an die Datenzentrale 2 übertragen.

Sobald die Datenzentrale 2 die Authentizität des ersten Datensatzes überprüft hat, sendet sie einen entsprechenden Bestätigungsdatensatz an das Fahrzeug 1. Dieser Bestätigungsdatensatz umfasst eine dem zweiten Sicherheitsmodul zugeordnete zweiten Sicherheitsmodulidentifikation. Die zweite Sicherheitsmodulidentifikation stellt dabei eine erste Empfängeridentifikation dar, die den Empfänger des ersten Datensatzes kennzeichnet.

Die erste Verarbeitungseinheit 1.3 schreibt diesen Bestätigungsdatensatz zusammen mit einem für den Zeitpunkt des Erhalts des Bestätigungsdatensatzes charakteristischen zweiten Zeitstempel in den vorhandenen ersten Datensatz und authentifiziert diesen dann wieder in der oben beschriebenen Weise, indem sie eine digitale Signatur über dem ersten Datensatz bildet. Diese digitale Signatur wird dann zusammen mit dem ersten Datensatzes in einen ersten Protokolldatensatz geschrieben, der dann in der oben beschriebenen Weise in den ersten Protokollspeicher 1.5 eingebracht wird.

Der erste Protokolldatensatz wird anschließend an die Datenzentrale 2 übermittelt, wo er nach entsprechender Überprüfung seiner Authentizität in einem mit dem zweiten Sicherheitsmodul 2.2 verbundenen zweiten Protokollspeicher 2.3 gespeichert wird. Es versteht

sich, dass die Datenzentrale 2 bei anderen Varianten der Erfindung auch einen solchen Protokolldatensatz selbst generieren und in den zweiten Protokollspeicher ablegen kann.

Dieser erste Protokolldatensatz authentifiziert somit in vorteilhafter Weise sowohl die Quellen und den Empfänger der jeweiligen Daten, bestimmte Erfassungs- und Verarbeitungszeitpunkte sowie die Übertragung selbst, sodass die mit diesen Daten verbundenen Sachverhalte zu einem späteren Zeitpunkt zweifelsfrei nachgewiesen werden können. Insbesondere ist es möglich, den Empfang der ersten Daten in der Datenzentrale 2 nachzuweisen.

Nach Erhalt und Überprüfung der Authentizität der ersten Daten in der Datenzentrale 2 werden diese alleine mit dem Sicherheitsmodul 2.2 verbundene Analyseeinrichtung 2.4 der Datenzentrale 2 übermittelt. Diese analysiert die übermittelten ersten Daten. Hierbei berücksichtigt die unter anderem statistische Daten, welche nicht von dem Fahrzeug 1 stammen.

Die Analyseeinrichtung 2.4 löst zum einen in Abhängigkeit von den übermittelten Kilometerwerten als erste Überwachungsreaktion einen ersten Abrechnungsvorgang für die gefahrenen Kilometer durch eine mit dem zweiten Sicherheitsmodul 2.2 verbundenes Abrechnungsmodul 2.5 als erster Überwachungsreaktionseinrichtung aus.

Als zweite Überwachungsreaktion löst die Analyseeinrichtung 2.4 in Abhängigkeit von der Analyse der ersten Daten die Generierung von Betriebsbeeinflussungsdaten für das Fahrzeug 1 durch eine mit dem zweiten Sicherheitsmodul 2.2 verbundene zweite Überwachungsreaktionseinrichtung 2.6 aus. Diese Betriebsbeeinflussungsdaten werden in einem weiteren ersten Datensatz von der Datenzentrale 2 über das Mobilfunknetz 3 an das Fahrzeug 1 übermittelt. Hierbei wird analog zu der oben beschriebenen Übermittlung der ersten Daten von dem Fahrzeug 1 zu Datenzentrale 2 verfahren, sodass diesbezüglich auf die obigen Ausführungen verwiesen wird. Insbesondere werden die ersten Daten in analoger Weise authentifizierten und es wird ein entsprechender Protokolldatensatz für die Übertragung generiert und sowohl im Fahrzeug 1 als auch in der Datenzentrale 2 gespeichert.

Die Betriebsbeeinflussungsdaten umfassen zum einen in Abhängigkeit von den übermittelten Kilometerwerten einen Hinweis über die aktuell gefahrenen Kilometer, den hierfür aktuellen Tarif sowie den aktuellen Abrechnungswert. Dieser Hinweis wird nach Verifizierung der Authentizität der Betriebsbeeinflussungsdaten im ersten Sicherheitsmodul 1.2 an eine mit dem ersten Sicherheitsmodul 1.2 verbundene Betriebsbeeinflussungseinrichtung 6 weitergegeben, welche diesen wiederum über ein damit verbundenes Display 7 an den Nutzer des Fahrzeugs 1 ausgibt. Die Betriebsbeeinflussungsdaten können weiterhin in Abhängigkeit von der Analyse der übermittelten Fahrzeugüberwachungsdaten (Motorölstand und Bremsenqua-

lität) im Falle des Drohens kritischer Zustände entsprechende Warnhinweise enthalten, die ebenfalls über das Display 7 an den Nutzer des Fahrzeugs 1 ausgegeben werden.

Schließlich löst die Analyseeinrichtung 2.4 als dritte Überwachungsreaktion in Abhängigkeit von der Analyse der ersten Daten die Durchführung eines Wartungsprotokolls für das Fahrzeug 1 durch eine mit dem zweiten Sicherheitsmodul 2.2 verbundene dritte Überwachungsreaktionseinrichtung in Form einer Fahrzeugmanagementeinrichtung 2.7 aus. Hierbei kann in Abhängigkeit von den Überwachungsdaten unter anderem die Wartung des Fahrzeuges 1 bei Rückgabe geplant und vorbereitet werden. Insbesondere können erforderliche Ersatzteile oder dergleichen bereits vorab bestellt werden, um die erforderliche Zeit für die Wartung so kurz wie möglich zu halten und damit die Ausfallzeiten des Fahrzeugs 1 zu verringern.

Die Erfassungseinrichtungen 4 und 5, das erste Sicherheitsmodul 1.2 und das erste Mobilfunkmodul 1.1 sind in einer vor unbefugtem Zugriff geschützten sicheren Umgebung 1.3 angeordnet, um den unbefugten Zugriff nicht nur auf die Daten des Sicherheitsmoduls ein vom zweiten sondern auch auf die Daten, die von und zu den Erfassungseinrichtungen 4 und 5 bzw. dem ersten Mobilfunkmodul 1.1 geliefert werden, wirksam zu unterbinden.

Die sichere Umgebung 1.3 wird zum einen physisch durch sichere Gehäuse der Erfassungseinrichtungen 4 und 5, des Mobilfunkmoduls 1.1 und des ersten Sicherheitsmoduls 1.2 hergestellt, die mit hinlänglich bekannten Mittel zur Erfassung von Manipulationen am Gehäuse ausgestattet sind. Zum anderen wird sie logisch durch ein entsprechend abgesichertes Kommunikationsprotokoll zwischen diesen Komponenten hergestellt. So wird bei jeder Kommunikation zwischen diesen Komponenten über eine entsprechend starke gegenseitige Authentifizierung ein gesicherter Kommunikationskanal aufgebaut. Es versteht sich, dass die Komponenten hierzu über entsprechende Kommunikationsmittel verfügen, welche die beschriebenen Sicherheitsfunktionalitäten zur Verfügung stellen.

Es versteht sich jedoch, dass bei anderen Varianten der Erfindung je nach den zu stellenden Sicherheitsanforderungen keine oder lediglich einzelne der genannten Komponenten in einer entsprechenden sicheren Umgebung angeordnet sein können.

Figur 3 zeigt ein weiteres bevorzugtes Ausführungsbeispiel der erfindungsgemäßen Anordnung, die in ihrer grundsätzlichen Funktion derjenigen aus Figur 1 gleicht, sodass hier lediglich auf die Unterschiede eingegangen werden soll.

Ein Unterschied besteht darin, dass es sich bei der mit dem ersten Sicherheitsmodul 1.2' verbundenen ersten Übertragungseinrichtung des Fahrzeugs 1' um eine kurzreichweitige

erste Infrarotschnittstelle 1.1' handelt. Die Infrarotschnittstelle 1.1' arbeitet dabei nach dem IrDA-Standard. Es versteht sich jedoch, dass bei anderen Varianten der Erfindung auch beliebige andere Übertragungsverfahren mit kurzer Reichweite, wie beispielsweise Bluetooth etc., verwendet werden können.

Die zweite Übertragungseinrichtung ist von einem Serviceterminal 8 gebildet. Dieses Serviceterminal 8 umfasst eine entsprechende zweite Infrarotschnittstelle 8.1 und ein damit verbundenes Kommunikationsmodul 8.2, welches die von der zweiten Infrarotschnittstelle 8.1 empfangenen ersten Daten über ein Telekommunikationsnetz 9 an die Datenzentrale 2' übermittelt.

Die Generierung, Authentifizierung, Übermittlung und Protokollierung der sicherheitsrelevanten ersten Daten von dem Fahrzeug 1' zur Datenzentrale 2' und umgekehrt erfolgt analog der oben in Zusammenhang mit Figur 1 beschriebenen Ausführungsform, sodass hier lediglich auf die obigen Ausführungen verwiesen wird.

Ein weiterer Unterschied besteht darin, dass das erste Sicherheitsmodul 1.2' mit einer Fahrzeugmanagementüberwachungseinrichtung 10 verbunden ist, die wiederum mit der Fahrzeugmanagementeinrichtung 11 des Fahrzeugs 1' verbunden ist. Die Fahrzeugmanagementeinrichtung 11 stellt dabei diejenige Einrichtung dar, welche die Funktionen der einzelnen Komponenten des Fahrzeugs steuert. Sie umfasst insbesondere das Motormanagement etc.

Die Fahrzeugmanagementüberwachungseinrichtung 10 überwacht in diesem Fall als dritte Erfassungseinrichtung unter anderem die Funktion der Softwarekomponenten der Fahrzeugmanagementeinrichtung 11. Die von der Fahrzeugmanagementüberwachungseinrichtung 10 erfassten Daten werden als dritte Erfassungswerte und damit als Überwachungsdaten in der oben beschriebenen Weise in einen ersten Datensatz eingebracht, authentifiziert und an die Datenzentrale 2' übermittelt.

In Abhängigkeit von der Analyse der übermittelten Überwachungsdaten in der Datenzentrale 2' generiert, authentifizierten und sendet die Datenzentrale 2' entsprechende Betriebsbeeinflussungsdaten in der oben beschriebenen Weise über das Serviceterminal 8 an das Fahrzeug 1'. Bei der Analyse der Überwachungsdaten überprüft die Datenzentrale 2' nicht nur die Integrität der Fahrzeugmanagementeinrichtung 11. Sie überprüft unter anderem auch die aktuelle Version der durch die Fahrzeugmanagementeinrichtung 11 verwendeten Softwaremodule. Existiert für eines der Softwaremodule eine neue Version, wird diese als Bestandteil der Betriebsbeeinflussungsdaten an das Fahrzeug 1' übersandt.

Nach dem das erste Sicherheitsmodul 1.2' die Authentizität der Betriebsbeeinflussungsdaten in der oben beschriebenen Weise verifiziert hat, gibt es die Betriebsbeeinflussungsdaten, insbesondere das neue Softwaremodul an die Fahrzeugmanagementüberwachungseinrichtung 10 weiter. Diese Fahrzeugmanagementüberwachungseinrichtung 10 stellt gleichzeitig eine Betriebsbeeinflussungseinrichtung dar, indem sie den Austausch des nichtmehr aktuellen alten Softwaremoduls durch das neue Softwaremodul in der Fahrzeugmanagementeinrichtung 11 steuert.

Auch die Übertragung der Betriebsbeeinflussungsdaten von der Datenzentrale 2' zum Fahrzeug 1 wird in der oben beschriebenen Weise protokolliert. Hierbei wird in den entsprechenden ersten Datensatz zudem eine Identifikation des Serviceterminals 8 als Quellenidentifikation aufgenommen, um auch die Übertragung über dieses Serviceterminal 8 zu einem späteren zweifelsfrei nachvollziehen zu können.

Insbesondere wird hier die Identifikation des ersten Sicherheitsmoduls 1.2' als Empfängeridentifikation in den ersten Datensatz des Protokolldatensatzes aufgenommen. Dies kann in Fällen, in denen der Austausch des betreffenden Softwaremoduls kostenpflichtig ist, später als Nachweis dienen, dass der Softwaremodul tatsächlich im Fahrzeug 1' empfangen wurde. Gegebenenfalls kann auch eine entsprechende Austauschbetätigung in den ersten Datensatz aufgenommen werden, um auch den tatsächlichen Austausch zweifelsfrei nachvollziehbar zu machen.

Es versteht sich, dass in solchen Fällen eines kostenpflichtigen Wartung der Fahrzeugsoftware oder auch bei anderen kostenpflichtigen Betriebsbeeinflussungen in der Datenzentrale mit Erhalt einer entsprechenden Empfangsbestätigung vom Fahrzeug 1' ein entsprechender Abrechnungsvorgang ausgelöst werden kann.

Die Kommunikation zwischen dem Fahrzeug 1' und der Datenzentrale 2' läuft wie die oben im Zusammenhang mit Figur 1 beschriebene Kommunikation ab. Insbesondere findet jeweils eine starke wechselseitige Authentifizierung unter Verwendung kryptographischer Mittel statt, sodass in Verbindung mit der Authentifizierung der ersten Daten jeweils gewährleistet ist, dass nur autorisierte und authentische Daten ausgetauscht und verwendet werden.

Mit dem beschriebenen Ausführungsbeispiel lässt sich beispielsweise ein flächendeckendes Netz von Serviceterminals 8 realisieren, über das eine einfache Überwachung und Fernwartung von Fahrzeugen möglich ist.

Das Ausführungsbeispiel wurde vorstehend anhand einer drahtlosen Verbindung zum Serviceterminal 8 beschrieben. Es versteht sich jedoch, dass bei anderen Varianten auch eine drahtgebundene Verbindung zum Serviceterminal vorgesehen sein kann, wie dies in Figur 3 durch den Pfeil 12 angedeutet ist. So kann beispielsweise ein Datenkabel verwendet werden, welches das Fahrzeug über entsprechende serielle Schnittstellen mit der zweiten Übertragungseinrichtung des Serviceterminals verbindet.

Weiterhin versteht es sich, dass es sich bei anderen Varianten der Erfindung bei dem Serviceterminal ebenfalls um eine mobile Einrichtung handeln kann, die dann gegebenenfalls über ein Mobilfunknetz oder dergleichen eine Verbindung zur Datenzentrale herstellt. Eine derartige Variante der Erfindung eignet sich besonders für den Einsatz in Zusammenhang mit Pannendiensten oder dergleichen.

Schließlich versteht es sich, dass das erste Sicherheitsmodul nicht notwendigerweise Bestandteil der mobilen Einheit sein muss. So ist es im Zusammenhang mit den soeben genannten Serviceterminals, insbesondere den mobilen Serviceterminals, möglich, das erste Sicherheitsmodul oder Teile davon, beispielsweise das Kryptographiemodul, in dem Serviceterminal zu integrieren. Dabei kann dann vorgesehen sein, dass die mobile Einrichtung beispielsweise neben den Erfassungseinrichtungen sowie einer entsprechenden Schnittstelle zur Verbindung mit dem Serviceterminal lediglich den ersten Protokollspeicher aufweist, in den der Protokolldatensatz durch das Serviceterminal geschrieben wird.

Figur 4 zeigt ein weiteres bevorzugtes Ausführungsbeispiel der erfindungsgemäßen Anordnung, die in ihrer grundsätzlichen Funktion derjenigen aus Figur 1 gleicht, sodass hier lediglich auf die Unterschiede eingegangen werden soll.

Ein Unterschied besteht darin, dass das erste Sicherheitsmodul 1.2" eines Lastkraftwagens als erstem Fahrzeug 1" über einen Fahrzeugdatenbus 13 nicht nur mit einer Erfassungseinrichtung 14 des Fahrzeugs 1" verbunden ist, über die Zustandsdaten des Fahrzeugs, unter anderem dessen Position, ermittelt werden. Vielmehr ist das erste Sicherheitsmodul 1.2" auch mit einer Erfassungseinrichtung 15.1 eines geladenen ersten Containers 15 und einer Erfassungseinrichtung 16.1 eines geladenen zweiten Containers 16 verbunden. Über die Erfassungseinrichtungen 15.1 und 16.1 werden jeweils Zustandsdaten des Containers 15 bzw. 16 und seiner Ladung erfasst.

Bei dem Fahrzeugdatenbus 13 handelt es sich im vorliegenden Fall um einen drahtlosen Datenbus. Es versteht sich jedoch, dass bei anderen Varianten der vorliegenden Erfindung auch ein drahtgebundener Datenbus verwendet werden kann.

Die Erfassungswerte der Erfassungseinrichtungen 14, 15.1 und 16.1 werden an das erste Sicherheitsmodul 1.2" weitergegeben und dann in der oben in Zusammenhang mit Figur 1 beschriebenen Weise über ein mit dem ersten Sicherheitsmodul 1.2" verbundenes erstes Mobilfunkmodul an eine - nicht dargestellte - entfernte Datenzentrale übermittelt.

Hiermit ist es nicht nur möglich, den Zustand des Fahrzeugs 1" zu überwachen und gegebenenfalls zu beeinflussen. Vielmehr ist es mit einem einzigen Sicherheitsmodul 1.2" auch möglich, den Zustand der Ladung des Fahrzeugs 1" zu überwachen und gegebenenfalls zu beeinflussen. Handelt es sich beispielsweise bei dem Container 15 um einen Kühlcontainer und wird über die Erfassungseinrichtung ein Anstieg der Temperatur im Container 15 über einen vorgegebenen Grenzwert ermittelt, so kann in der oben beschriebenen Weise über die Datenzentrale eine Betriebsbeeinflussung erfolgen. Hierzu kann beispielsweise durch entsprechende von der Datenzentrale übermittelte Betriebsbeeinflussungsdaten die Kühlleistung des Kühlaggregats 15.2 des Containers 15 erhöht werden. Zudem kann durch die gespeicherten und in der oben beschriebenen Weise authentifizierten Protokolldatensätze gegebenenfalls zweifelsfrei der Temperaturverlauf im Inneren des Containers 15 nachgewiesen werden. Dies kann beispielsweise beim Transport von verderblichen Lebensmitteln, wie Fleisch oder dergleichen, dazu verwendet werden, nachzuweisen, dass die Temperatur der Lebensmittel für die Zeit, die sie im Inneren des Containers 15 aufbewahrt wurden, stets unterhalb vorgeschriebener Grenzwerte lag.

Weiterhin ist es durch die Ermittlung der Position des Fahrzeugs 1" durch die Erfassungseinrichtung 14 insbesondere möglich, den Standort der Container 15 und 16 nachzuvollziehen. Insbesondere können diese Erkenntnisse in eine übergeordnete Logistikplanung einfließen.

Die Positionsbestimmung durch die Erfassungseinrichtung 14 kann in beliebiger bekannter Weise erfolgen. So kann die Erfassungseinrichtung 14 ein entsprechendes GPS-Modul. Ebenso kann aber auch in bekannter Weise eine Positionsbestimmung über das Mobilfunknetz 3" erfolgen.

Auch hier sei erwähnt, dass die Kommunikation zwischen dem Fahrzeug 1" und der Datenzentrale wie die oben im Zusammenhang mit Figur 1 beschriebene Kommunikation abläuft. Insbesondere findet jeweils eine starke wechselseitige Authentifizierung unter Verwendung kryptographischer Mittel statt, sodass in Verbindung mit der Authentifizierung der ersten Daten jeweils gewährleistet ist, dass nur autorisierte und authentische Daten ausgetauscht und verwendet werden.

Die vorliegende Erfindung wurde vorstehend ausschließlich anhand von Beispielen für Fahrzeuge beschrieben. Es versteht sich jedoch, dass Erfindung auch im Zusammenhang mit beliebigen anderen beweglichen Einrichtungen, wie beispielsweise Containern etc. zur Anwendung kommen kann.

*****

Patentansprüche

1. Verfahren zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung (1; 1'; 1"), insbesondere einem Fahrzeug, und einer von der ersten Einrichtung (1; 1'; 1") zumindest zeitweise entfernten Datenzentrale (2; 2'), wobei die Übertragung der Daten über wenigstens eine mobile erste Übertragungseinrichtung (1.1; 1.1'; 1.1") erfolgt, dadurch gekennzeichnet, dass die übertragenen Daten erste Daten umfassen, die durch kryptographische Mittel authentifiziert werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die ersten Daten zur Authentifizierung einer ersten Quelle (1.2, 4, 5; 8) der ersten Daten eine erste Quellenidentifikation umfassen.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die ersten Daten zur Authentifizierung eines ersten Empfängers (2.2) der ersten Daten eine erste Empfängeridentifikation umfassen.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Daten zur Authentifizierung der Übertragung der ersten Daten eine Übertragungsidentifikation umfassen.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Daten wenigstens eine für ein vorgebbares Ereignis charakteristische Zeitkennung umfassen.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die authentifizierten ersten Daten in einen Protokolldatensatz eingefügt werden, der in der ersten Einrichtung (1; 1'; 1") und/oder der Datenzentrale (2; 2') gespeichert wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Daten unter Verwendung wenigstens einer ersten digitalen Signatur authentifiziert werden.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Daten von der ersten Einrichtung (1; 1'; 1") zur Datenzentrale (2; 2') übertragene erste Überwachungsdaten umfassen, die wenigstens einen ersten Er-

fassungswert einer ersten Erfassungsgröße umfassen, der von einer ersten Erfassungseinrichtung (4, 5; 10; 14, 15.1, 16.1) der ersten Einrichtung (1; 1'; 1") erfasst wurde.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass die erste Erfassungsgröße eine Zustandsgröße der ersten Einrichtung (1; 1'; 1") ist.

10. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Daten wenigstens Betriebsbeeinflussungsdaten umfassen, die zur Beeinflussung des Betriebs der ersten Einrichtung (1; 1'; 1") an die erste Einrichtung (1; 1'; 1") übermittelt werden.

11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Daten über wenigstens eine zweite Datenübertragungseinrichtung (3.1; 8.2) übertragen werden.

12. Verfahren zur Überwachung einer mobilen ersten Einrichtung, insbesondere eines Fahrzeugs, bei dem zwischen der mobilen ersten Einrichtung (1; 1'; 1") und einer von der ersten Einrichtung (1; 1'; 1") zumindest zeitweise entfernten Datenzentrale (2; 2') über wenigstens eine mobile erste Übertragungseinrichtung (1.1; 1.1'; 1.1") erste Daten mit einem Verfahren nach einem der vorhergehenden Ansprüche übertragen werden, dadurch gekennzeichnet, dass die ersten Daten von der ersten Einrichtung (1; 1'; 1") zur Datenzentrale (2; 2') übertragene erste Überwachungsdaten umfassen, wobei

- die ersten Überwachungsdaten wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße umfassen, der von einer ersten Erfassungseinrichtung (4, 5; 10; 14, 15.1, 16.1) der ersten Einrichtung erfasst wurde,

- die ersten Überwachungsdaten in der Datenzentrale (2; 2') verifiziert werden und

- die ersten Überwachungsdaten bei erfolgreicher Verifikation in der Datenzentrale (2; 2') analysiert werden.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass in der Datenzentrale (2; 2') in Abhängigkeit von der Analyse der ersten Überwachungsdaten eine erste Überwachungsreaktion ausgelöst wird.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass die erste Überwachungsreaktion einen Abrechnungsvorgang umfasst.

15. Verfahren nach Anspruch 13 oder 14, dadurch gekennzeichnet, dass die erste Überwachungsreaktion die Generierung von Betriebsbeeinflussungsdaten umfasst, die zur Beeinflussung des Betriebs der ersten Einrichtung (1; 1'; 1") an die erste Einrichtung (1; 1'; 1") übermittelt werden.

16. Verfahren nach einem der Ansprüche 13 bis 15, dadurch gekennzeichnet, dass bei der Analyse weitere, nicht von der ersten Einrichtung (1; 1'; 1") übermittelte Daten berücksichtigt werden.

17. Anordnung zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung, insbesondere einem Fahrzeug, und einer von der ersten Einrichtung (1; 1'; 1") zumindest zeitweise entfernten Datenzentrale (2; 2'), wobei zur Übertragung der Daten wenigstens eine mobile erste Übertragungseinrichtung (1.1; 1.1'; 1.1") vorgesehen ist, dadurch gekennzeichnet, dass die übertragenen Daten erste Daten umfassen und wenigstens eine Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2") vorgesehen ist, die zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet ist.

18. Anordnung nach Anspruch 17, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2") zur Authentifizierung einer ersten Quelle (1.2, 4, 5; 8) der ersten Daten zum Einbringen einer ersten Quellenidentifikation in den ersten Datensatz ausgebildet ist.

19. Anordnung nach Anspruch 17 oder 18, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2") zur Authentifizierung eines ersten Empfängers (2.2) der ersten Daten zum Einbringen einer ersten Empfängeridentifikation in den ersten Datensatz ausgebildet ist.

20. Anordnung nach einem der Ansprüche 17 bis 19, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2; 1.2'; 1.2") zur Authentifizierung der Übertragung der ersten Daten zum Einbringen einer Übertragungsidentifikation in den ersten Datensatz ausgebildet ist.

21. Anordnung nach einem der Ansprüche 17 bis 20, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2") zum Einbringen wenigstens einer für ein

vorgebbares Ereignis charakteristischen Zeitkennung in den ersten Datensatz ausgebildet ist.

22. Anordnung nach einem der Ansprüche 17 bis 21, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2") zum Einbringen der authentifizierten ersten Daten in einen Protokolldatensatz ausgebildet ist und dass die erste Einrichtung (1; 1'; 1") einen ersten Protokollspeicher (1.5) zum Speichern des Protokolldatensatzes aufweist und/oder die Datenzentrale (2; 2') einen zweiten Protokollspeicher (2.3) zum Speichern des Protokolldatensatzes aufweist.

23. Anordnung nach einem der Ansprüche 17 bis 22, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2") zur Bildung einer ersten digitalen Signatur unter Verwendung der ersten Daten ausgebildet ist.

24. Anordnung nach einem der Ansprüche 17 bis 23, dadurch gekennzeichnet, dass die erste Einrichtung (1; 1'; 1") eine erste Sicherheitseinrichtung (1.2; 1.2'; 1.2") umfasst und/oder die Datenzentrale (2; 2') eine zweite Sicherheitseinrichtung (2.2) umfasst.

25. Anordnung nach einem der Ansprüche 17 bis 24, dadurch gekennzeichnet, dass die ersten Daten von der ersten Einrichtung (1; 1'; 1") zur Datenzentrale (2; 2') übertragene erste Überwachungsdaten umfassen, die wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße umfassen, wobei die erste Einrichtung eine erste Erfassungseinrichtung (4, 5; 10; 14, 15.1, 16.1) zur Erfassung des ersten Erfassungswerts umfasst.

26. Anordnung nach Anspruch 25, dadurch gekennzeichnet, dass die erste Erfassungseinrichtung (4, 5; 10; 14, 15.1, 16.1) zur Erfassung einer Zustandsgröße der ersten Einrichtung (1; 1'; 1") als erster Erfassungsgröße ausgebildet ist.

27. Anordnung nach einem der Ansprüche 17 bis 26, dadurch gekennzeichnet, dass die ersten Daten von der Datenzentrale (2; 2') zur ersten Einrichtung (1; 1'; 1") übertragene Betriebsbeeinflussungsdaten umfassen, wobei die erste Einrichtung (1; 1'; 1") eine Betriebsbeeinflussungseinrichtung (6; 10; 15.1) zur Beeinflussung des Betriebs der ersten Einrichtung (1; 1'; 1", 15) in Abhängigkeit von den Betriebsbeeinflussungsdaten aufweist.

28. Anordnung nach einem der Ansprüche 17 bis 27, dadurch gekennzeichnet, dass zur Datenübertragung zwischen der ersten Einrichtung (1; 1') und der Datenzentrale (2; 2') wenigstens eine zweite Datenübertragungseinrichtung (3.1; 8.2) vorgesehen ist.

29. Anordnung zur Überwachung einer mobilen ersten Einrichtung, insbesondere eines Fahrzeugs, mit einer Anordnung zur Übertragung von ersten Daten nach einem der Ansprüche 17 bis 28, dadurch gekennzeichnet, dass

- die ersten Daten von der ersten Einrichtung (1; 1'; 1") zur Datenzentrale übertragene (2; 2') erste Überwachungsdaten umfassen, die wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße umfassen, wobei die erste Einrichtung (1; 1'; 1") eine erste Erfassungseinrichtung (4, 5; 10; 14, 15.1, 16.1) zur Erfassung des ersten Erfassungswerts umfasst,

- die Datenzentrale (2; 2') eine zweite Sicherheitseinrichtung (2.2) zum Verifizieren der ersten Überwachungsdaten aufweist und

- die Datenzentrale (2; 2') eine mit der zweiten Sicherheitseinrichtung (2.2) verbundene Analyseeinrichtung (2.4) zum Analysieren der ersten Überwachungsdaten in Abhängigkeit vom Ergebnis der Verifikation aufweist.

30. Anordnung nach Anspruch 29, dadurch gekennzeichnet, dass wenigstens eine mit der Analyseeinrichtung (2.4) verbindbare Überwachungsreaktionseinrichtung (2.5, 2.6, 2.7) zur Durchführung einer ersten Überwachungsreaktion vorgesehen ist und die Analyseeinrichtung (2.4) zum Ansteuern der Überwachungsreaktionseinrichtung (2.5, 2.6, 2.7) zum Auslösen einer ersten Überwachungsreaktion in Abhängigkeit vom Ergebnis der Analyse der ersten Überwachungsdaten ausgebildet ist.

31. Anordnung nach Anspruch 30, dadurch gekennzeichnet, dass als Überwachungsreaktionseinrichtung eine mit der Analyseeinrichtung (2.4) verbindbare Abrechnungseinrichtung (2.5) vorgesehen ist.

32. Anordnung nach Anspruch 30 oder 31, dadurch gekennzeichnet, dass

- die Überwachungsreaktionseinrichtung (2.6, 2.7) zur Generierung von Betriebsbeeinflussungsdaten zur Beeinflussung des Betriebs der ersten Einrichtung (1; 1'; 1", 15) als erste Überwachungsreaktion ausgebildet ist,

- die Datenzentrale (2; 2') zur Übertragung erster Daten an die erste Einrichtung (1; 1'; 1") ausgebildet ist, wobei die ersten Daten die Betriebsbeeinflussungsdaten umfassen, und

- die erste Einrichtung (1; 1'; 1") eine Betriebsbeeinflussungseinrichtung (6; 10; 15.1) zur Beeinflussung des Betriebs der ersten Einrichtung in Abhängigkeit von den Betriebsbeeinflussungsdaten aufweist.

33. Anordnung nach Anspruch 32, dadurch gekennzeichnet, dass

- die erste Einrichtung (1; 1'; 1") eine erste Sicherheitseinrichtung (1.2; 1.2'; 1.2") umfasst, die zum Verifizieren der die Betriebsbeeinflussungsdaten umfassenden ersten Daten ausgebildet ist und

- die Betriebsbeeinflussungseinrichtung (6; 10; 15.1) zur Beeinflussung des Betriebs der ersten Einrichtung (1; 1'; 1", 15) in Abhängigkeit vom Ergebnis der Verifizierung ausgebildet ist.

34. Anordnung nach einem der Ansprüche 29 bis 33, dadurch gekennzeichnet, dass die Analyseeinrichtung (2.4) zur Berücksichtigung weiterer, nicht von der ersten Einrichtung übermittelter Daten ausgebildet ist.

35. Mobile erste Einrichtung, insbesondere Fahrzeug, für eine Anordnung nach einem der Ansprüche 17 bis 34, gekennzeichnet durch eine erste Datenübertragungseinrichtung (1.1; 1.1'; 1.1") zur Übertragung erster Daten und eine mit der ersten Datenübertragungseinrichtung (1.1; 1.1'; 1.1") verbindbare erste Sicherheitseinrichtung (1.2; 1.2'; 1.2"), die zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet ist.

36. Mobile erste Einrichtung nach Anspruch 35, dadurch gekennzeichnet, dass die erste Sicherheitseinrichtung (1.2; 1.2'; 1.2") zur Authentifizierung der ersten Datenübertragungseinrichtung (1.1; 1.1'; 1.1") zum Einbringen einer der ersten Datenübertragungseinrichtung (1.1; 1.1'; 1.1") zugeordneten Identifikation in den ersten Datensatz ausgebildet ist.

37. Datenzentrale für eine Anordnung nach einem der Ansprüche 17 bis 34, gekennzeichnet durch eine Datenübertragungseinrichtung (2.1) zur Übertragung erster Da-

ten und eine mit der Datenübertragungseinrichtung (2.1) verbindbare zweite Sicherheitseinrichtung (2.2), die zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet ist.

* * * * *

Zusammenfassung

Verfahren zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung (1; 1'; 1"), insbesondere einem Fahrzeug, und einer von der ersten Einrichtung (1; 1'; 1") zumindest zeitweise entfernten Datenzentrale (2; 2'), wobei die Übertragung der Daten über wenigstens eine mobile erste Übertragungseinrichtung (1.1; 1.1'; 1.1") erfolgt und die übertragenen Daten erste Daten umfassen, die durch kryptographische Mittel authentifiziert werden.

Figur 1

* * * * *

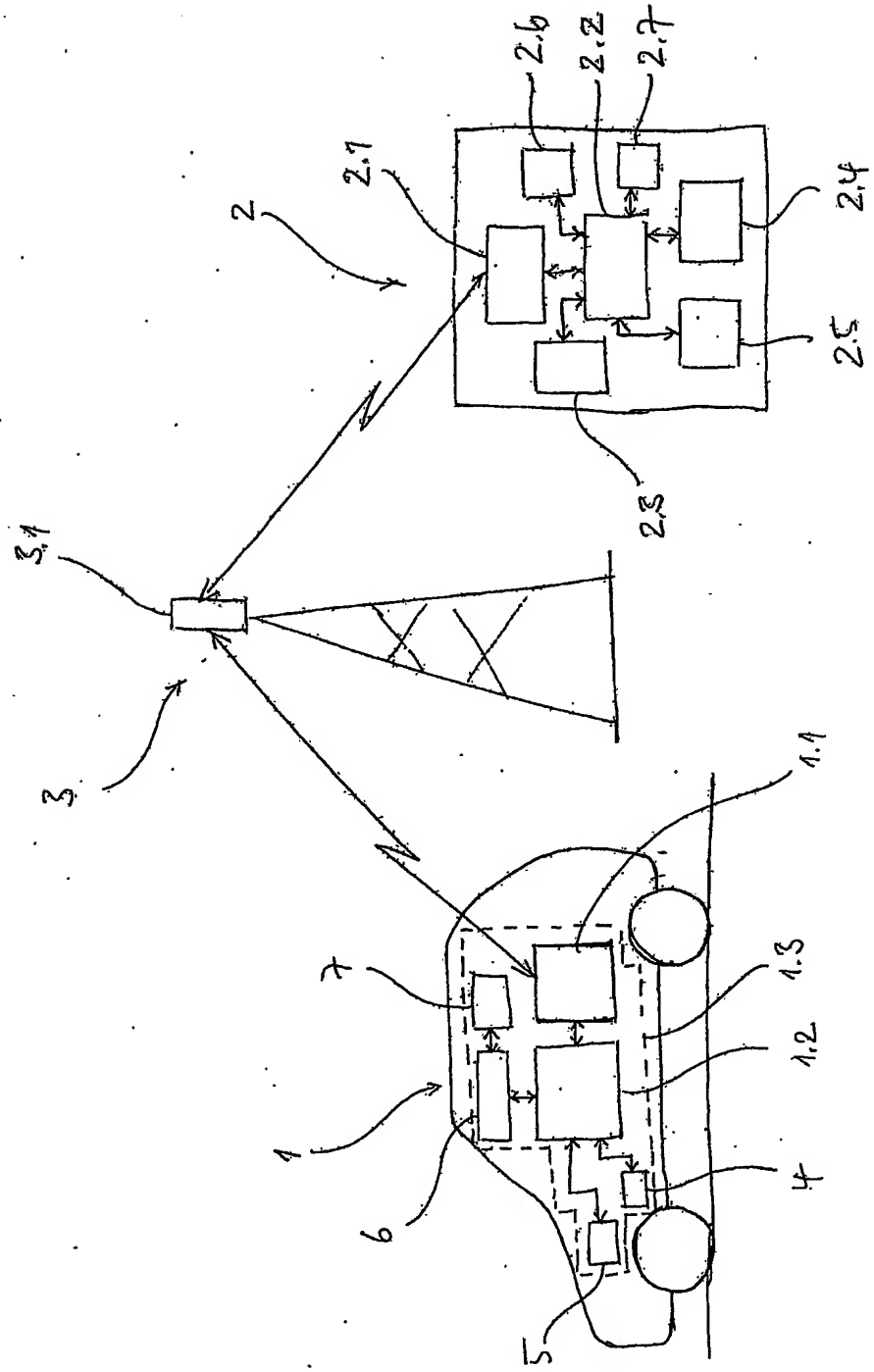

Fig. 1

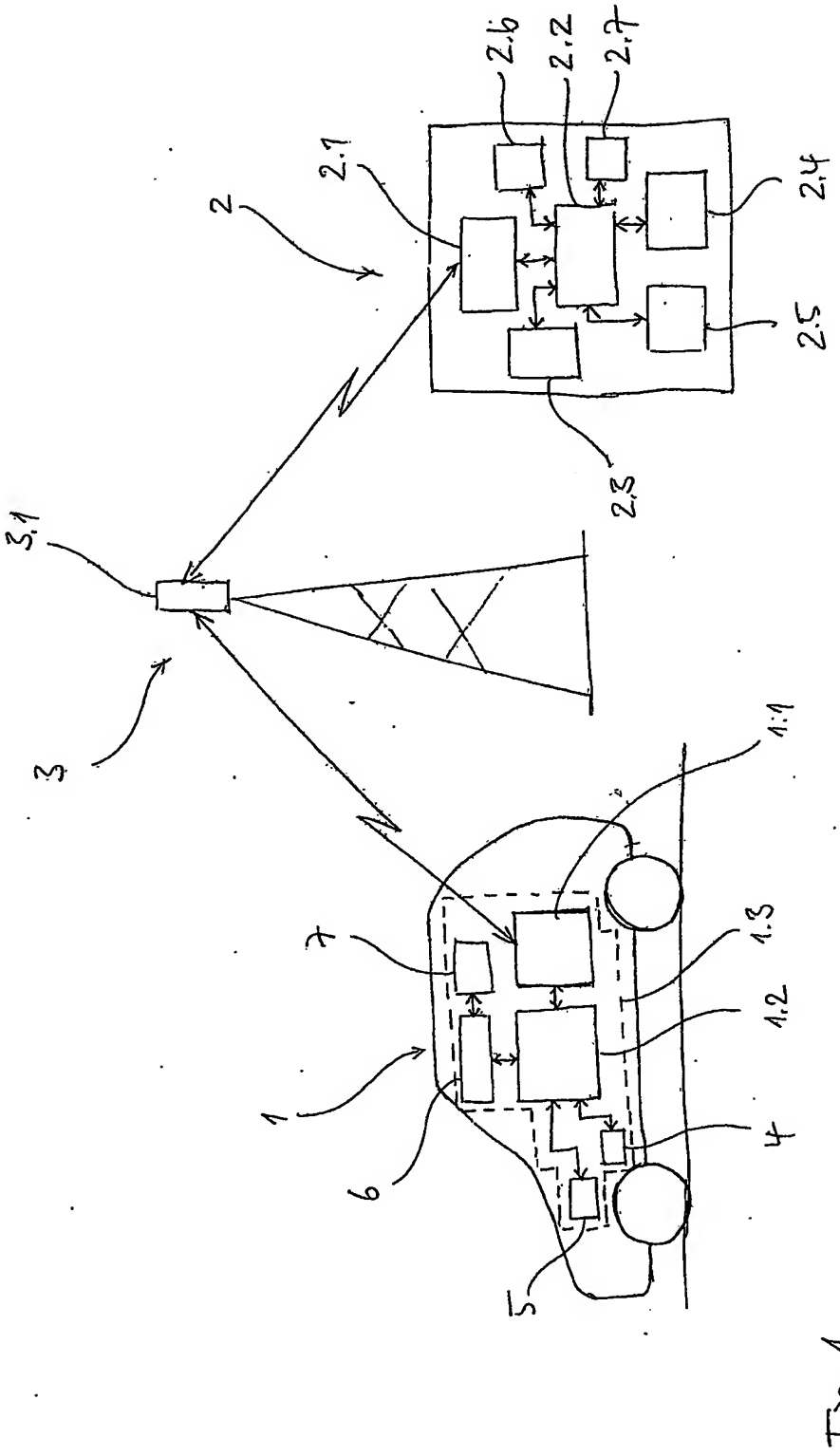

Fig. 1

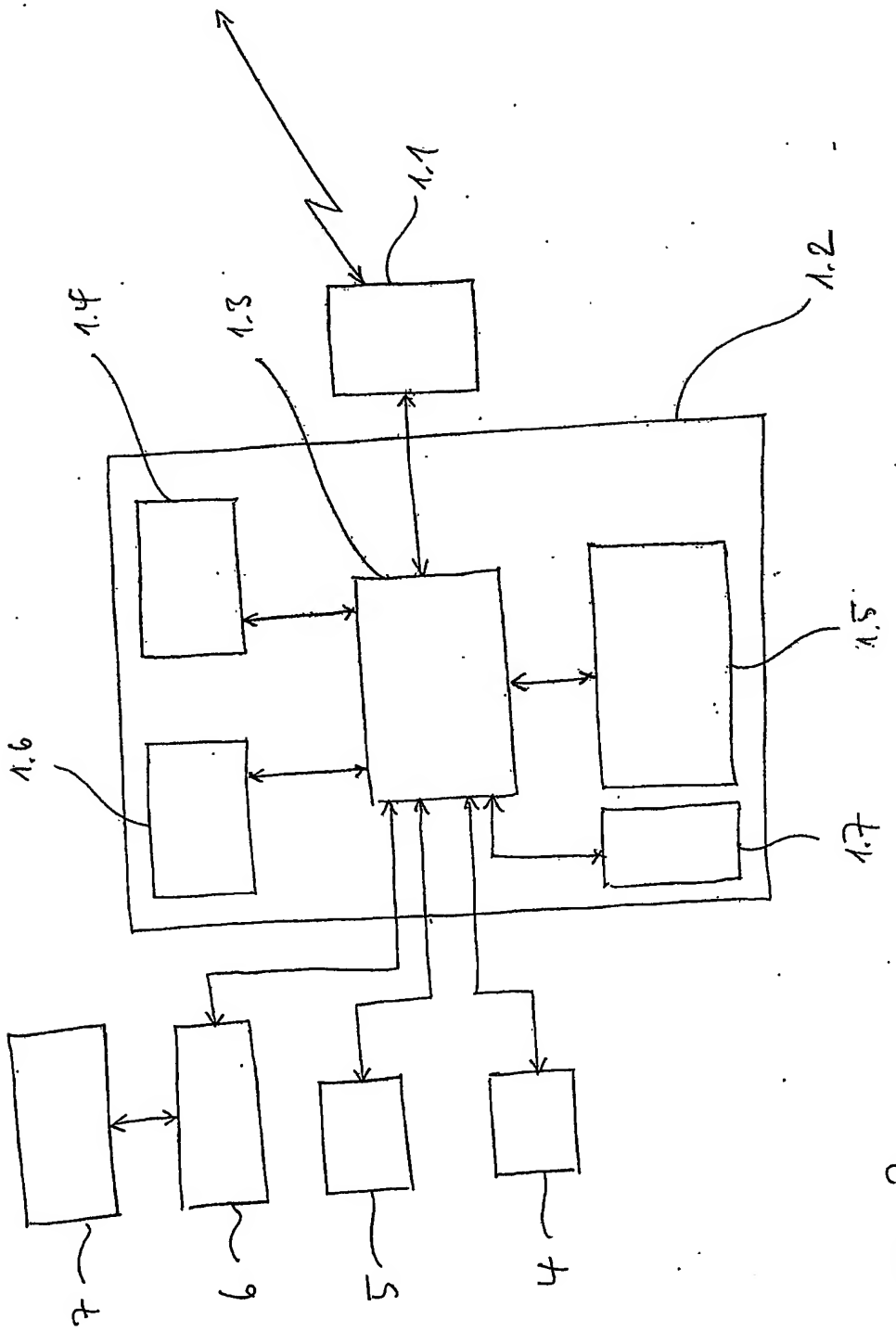

Fig. 2

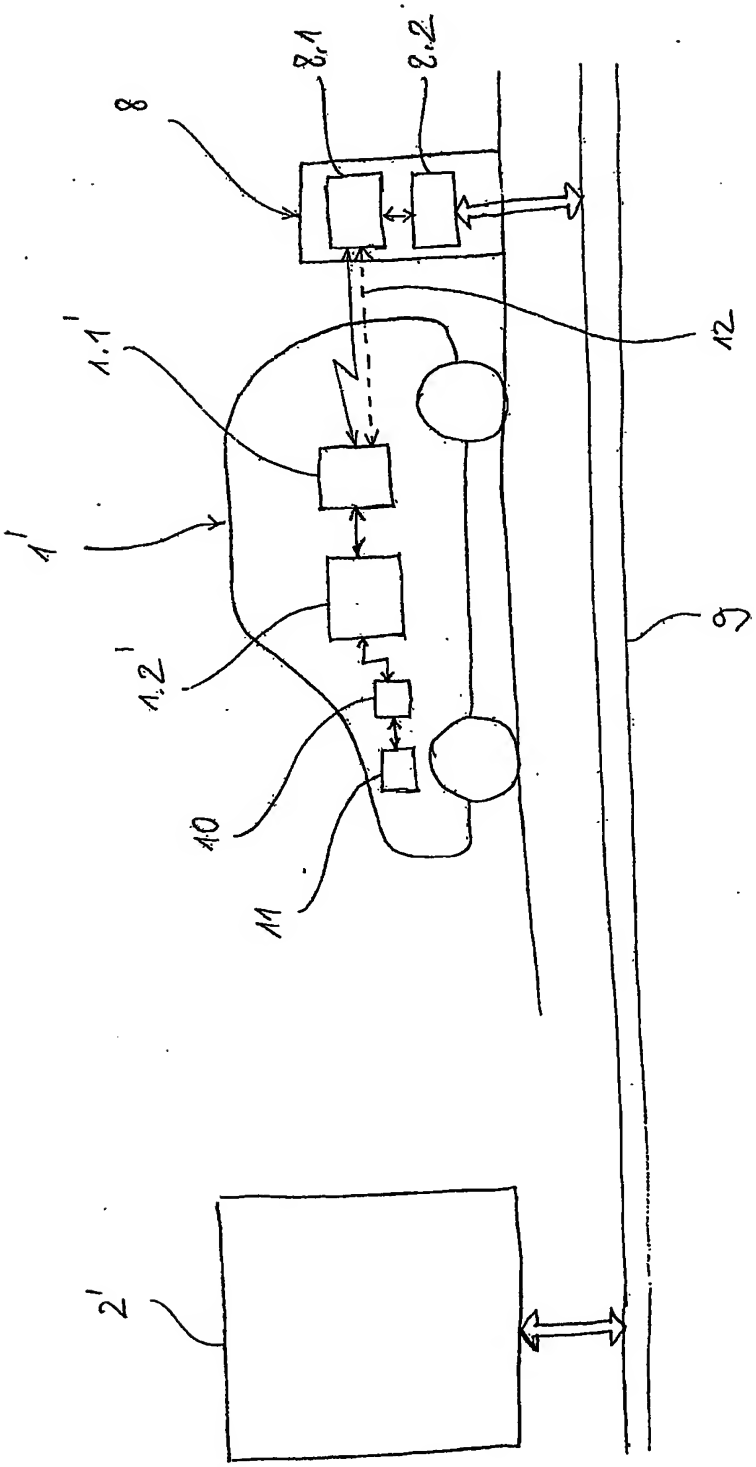

Fig. 3

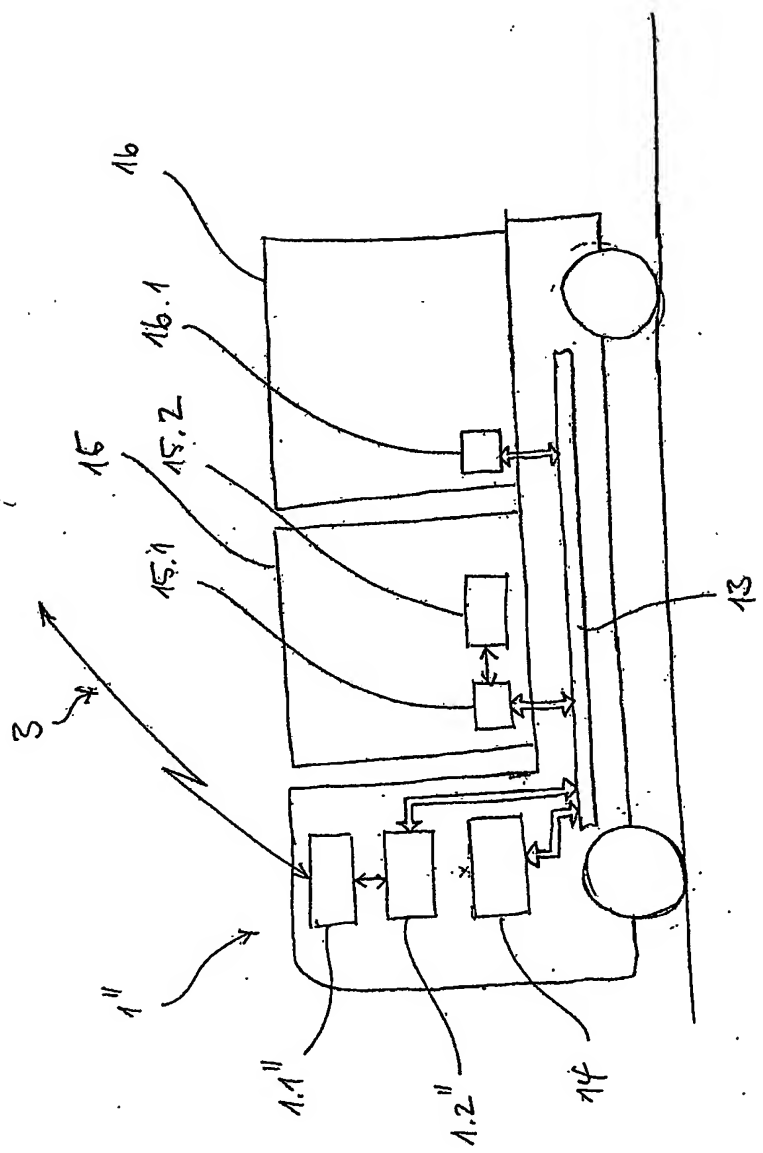

Fig. 4